

# DATA CENTER DISASTER RECOVERY & MAJOR INCIDENT MANAGEMENT

LAHTI UNIVERSITY OF APPLIED  
SCIENCES  
Degree Programme in Information  
and Communications Technology  
Master's Thesis  
Autumn 2017  
Aliisa Partio

Lahti University of Applied Sciences  
Master's Degree Programme in Information and Communications  
Technology

PARTIO, ALIISA:

Data center Disaster Recovery &  
Major Incident Management

Master's Thesis in Information and Communications Technology, 70  
pages

Autumn 2017

## ABSTRACT

---

The current IT world is becoming more virtualized, more 24/7, more user oriented. There has been a birth for a whole new requirement set for companies and organizations to ensure their environments are always working. Having systems always up and running is a necessity for many organizations, which in turn has brought forth clear demand for working disaster recovery solutions. People expect things to just be working all the time and for example web-sites with information of a system downtime, are becoming a thing from the past.

Disaster recovery and major incident management have become cornerstones for many companies' livelihood. Without working systems, the companies may lose a lot of revenue, even be faced with a situation where they need to close their operations completely. Even companies that do not suffer financially might suffer a huge blow to their image when the information customers are seeking is not ready right away.

Study aims to provide insight to one type of a data center environment and how to build a disaster recovery for most critical systems by using predictive research method. Alongside this, the goal is to find out how to manage the interconnected major incident process from a technical perspective.

The research provided insight that disaster recovery and major incident management are not solely a technical venture, they present a common goal for the whole organization and they require everyone to adapt and evolve to new ways of working. Result of the case study was a functional disaster recovery data center that allows future growth.

Key words: data center, disaster recovery, major incident management, business continuity, VMWare, Veeam

Lahden ammattikorkeakoulu  
Master's Degree Programme in Information and Communications  
Technology

PARTIO, ALIISA:

Datacenterin palautumissuunnitelma  
& Katastrofitilanteen hallinta

Master's Thesis in Information and Communications Technology, 70 sivua

Syksy 2017

## TIIVISTELMÄ

---

Nykyinen tietoyhteiskunta on muuttumassa enemmän virtuaaliseksi, enemmän 24/7 luonteiseksi ja enemmän käyttäjälähtöiseksi. Yritykset ja organisaatiot ovat saaneet vastaan uudenlaisia vaatimuksia, jotka edellyttävät jatkuvaa käytettävyyttä. Organisaatiot elävät periaatteella, että heidän palvelunsa ovat jatkuvasti käytettävissä, mikä on puolestaan luonut tarpeen rakentaa toimiva palautumissuunnitelma. On olemassa oletus, että tietojärjestelmät toimivat aina, ja aiemmin verkkosivuilla olleet ilmoitukset käynnissä olevasta käyttökatkosta ovat muuttumassa historian havinaksi.

Katastrofi- ja palautussuunnitelmat ovat muodostuneet monen yrityksen kulmakiviksi. Ilman toimivaa tietojärjestelmää, uhkaa yrityksiä liiketappiot ja pahimmassa tapauksessa jopa liiketoiminnan loppuminen. Yritykset jotka eivät kärsi taloudellisesti, voivat kärsiä jatkossa imago ongelmista tietojärjestelmän ongelman vuoksi.

Opinnäytetyö pyrkii kuvaamaan yhdenlaisen datacenter ympäristön ja miten tähän ympäristöön luodaan palautumissuunnitelma kriittisimmille komponenteille käyttäen ennustavaa tutkimusmenetelmää. Tämän lisäksi on tarkoitus löytää tekninen toimintamalli katastrofitilanteisiin.

Tutkimus tuotti tulokseksi, etteivät katastrofi- ja palautussuunnitelma tule toimimaan pelkästään teknisinä ponnistuksina, vaan ne vaativat koko organisaation tuen. Organisaation tulee kyetä sopeutumaan ja kehittymään uudenlaisiin toimintamalleihin. Tämän tutkielman tuloksena syntyi toimiva katastrofipalautumiseen käytettävä datacenteri, joka sallii tulevaisuudessa tapahtuvan kasvun.

Avainsanat: data center, palautumissuunnitelma, katastrofitilanteen hallinta, liiketoiminnan jatkuvuus, VMWare, Veeam

## CONTENTS

1	INTRODUCTION	1
1.1	Research objectives and research questions	2
1.2	Research methods	3
2	DATA CENTER ENVIRONMENT AND BUSINESS REQUIREMENTS	5
2.1	Data center environment	5
2.2	Data center business requirements	6
3	MODERN DATA CENTER	9
3.1	Data center standard comparison	11
3.2	Site selection	12
3.3	Space planning	13
3.3.1	Rack space	14
3.3.2	Electricity	14
3.3.3	Network cabling	15
3.3.4	Temperature & cooling	17
3.3.5	Fire suppression	18
3.3.6	Lighting	20
3.3.7	Supporting spaces	20
3.3.8	Access control	21
3.4	Architectural issues	22
3.4.1	Reliability	22
3.4.2	Availability	23
3.4.3	Labeling	24
4	DISASTER RECOVER AND MAJOR INCIDENT MANAGEMENT	25
4.1	Disaster recovery facilities	25
4.2	Disaster recovery plan	26
4.2.1	Using the disaster recovery plan	29
4.2.2	Testing the disaster recovery plan	30
4.3	Major Incident Management	31
4.3.1	Major Incident definition	31
4.3.2	Major Incident standards and best practises	31
4.3.3	Major Incident process	33
5	CASE STUDY	35

5.1	Research approach	35
5.2	Data collection	36
5.3	Background and design	39
5.3.1	Background	39
5.3.2	External datacenter design	41
5.3.3	Internal datacenter design	42
5.4	Cluster with shared storage	45
5.4.1	Cluster storage configuration	47
5.4.2	Cluster network configuration	48
5.5	Disaster recovery	50
5.6	Disaster recovery RTO, RPO and testing	53
5.7	Documentation	58
6	CONCLUSIONS	59
6.1	Case study result analysis	59
6.2	Research questions and discussion	60
	REFERENCES	64

## LIST OF ABBREVIATIONS

**ASHP** Air source heat pump. System which transfers heat from outside to inside a building, or vice versa.

**BCP** Business continuity plan. Process of creating systems of prevention and recovery to deal with potential threats to a company or an organization.

**BIA** Business Impact Analysis. Differentiates critical (urgent) and non-critical (non-urgent) organization functions/activities.

**DR** Disaster recovery. Involves a set of policies and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.

**DRP** Disaster recovery plan. Documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster.

**HVAC** Heating, ventilation and air conditioning. Technology of indoor and vehicular environmental comfort. Its goal is to provide thermal comfort and acceptable indoor air quality

**ICT** Information and communication technology. An extended term for information technology (IT) which stresses the role of unified communications and in the technologies, that provide access to information through telecommunications.

**IT** Information Technology. The use of any computers, storage, networking and other physical devices, infrastructure and processes to create, process, store, secure and exchange all forms of electronic data.

**LED** Light emitting diode. An electronic semiconductor device that emits light when electric current passes through it.

**LUN** Logical unit number. Number used to identify a logical unit, which is a device addressed by the SCSI protocol or Storage Area Network protocols which encapsulate SCSI, such as Fibre Channel or iSCSI.

**MIM** Major incident management. Process for handling major incident, which is the highest-impact, highest-urgency incident.

**PDU** Power distribution units. Device for controlling electrical power in a data center.

**RAID** Redundant array of independent disks. Data storage virtualization technology that combines multiple physical disk drive components into a single logical unit for the purposes of data redundancy, performance improvement, or both.

**ROI** Return on Investment. Measures the amount of return on an investment relative to the investment's cost

**RPO** Recovery point objective. Maximum targeted period in which data might be lost from an IT service due to a major incident.

**RTO** Recovery time objective. The targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) to avoid unacceptable consequences associated with a break in business continuity.

**SCSI** Small Computer System Interface. Set of standards for physically connecting and transferring data between computers and peripheral devices.

**SLA** Service-level agreement. Contract between a service provider (either internal or external) and the end user that defines the level of service expected from the service provider.

**SRT** System recovery time. Time until a system is operational after an incident.

**UPS** Uninterrupted Power System. Electrical apparatus that provides emergency power to a load when the input power source or mains power fails.

**VDS** vSphere Distributed Switch. VMware technology which provides a centralized interface from which you can configure, monitor and administer virtual machine access switching for the entire data center.

**WAN** Wide Area Network. Telecommunications network or computer network that extends over a large geographical distance.

## 1 INTRODUCTION

Modern data center infrastructure enables companies robust and maintenance free environment to run their business applications. To keep business running around the clock, new data centers need to be designed in a way that they are reliable, cost effective and flexible in order to meet the business requirements. In addition to running daily services, many companies have turned their sights to disaster recovery (DR) and major incident management (MIM), to ensure no revenue is lost in a case of a disaster.

In today's virtualized environments, the physical platform needs to be as flexible as its virtual counterpart. This provides a challenge for today's information and communication technology (ICT) professionals, as they need to ensure the business can keep on working based on pre-agreed parameters. Having well designed processes enables ICT professionals to plan and make decisions to ensure business continuity. As business criticality increases, having foresight for future investments is something that is desired from the ICT professionals.

Data centers built for disaster recovery purposes rely heavily on major incident management. Organization in question was looking for a data center solution to match their current MIM process. Based on the available documentation a new data center was to be built that would follow the industry standards as well as the organizations internal standards to ensure the best possible solution for business continuity.



## 1.1 Research objectives and research questions

The organization in question had identified the need for business continuity planning. They had placed two key development points for their ICT services, which were disaster recovery and major incident management. Organization had identified a need for more sustainable and faster recovery times and a need for disaster recovery site other than Microsoft Azure which they were already partly utilizing.

At the same time business processes for major incident management were also being built, so there was a need to specify technical model based on the common disaster recovery model. This set a requirement for the ICT to describe the business responsibilities during a technical recovery process.

Following research questions for the case study were based on the business requirements:

*How to ensure business critical service continuity within data center platform?*

*Which technical solution for data center platform should be utilized and where?*

*How long will it take to implement identified solutions?*

*How to make a common service model for all business units for business continuity?*

*How to ensure documentation is always up to date regarding business continuity?*

## 1.2 Research methods

The end-result to which this research aimed for was clear, build a data center to support business continuity. The design parameters, also known as limiting factors, were time and resources. Based on this information design science was chosen as the primary research method.

Design Science Research (DSR) “creates and evaluates IT artifacts intended to solve identified organizational problems”. (Hevner, Chatterjee 2010,271.) The process cycle for design science is visualized in figure 1. The cycle is split into five steps: awareness of problem, suggestion, development, evaluation, conclusion. This cycle was used to handle the whole case. The case study part relies on predictive research method, which is explained in chapter 5.1.



FIGURE 1. The design science cycle originally proposed by Takeda et al. (Kuechler & Vaishnavi 2008)

Awareness of problem in this study came from the business continuity requirement set by the organization. The proposal was to build a disaster recovery solution and gather the necessary material to handle major incident management. The research questions were used as a basis to achieve the best possible outcome.

Suggestion phase was introducing the suggested proposal to the organization and to get an acceptance for the project. Few different suggestions were presented to the organization before moving onto the actual development part of the cycle.

Once the timeline and resources were set by the project, the actual development could start. Building the actual data center was the main part of the development step. This part also utilizes the previously mentioned predictive research method.

After all the hardware and software components had been chosen and implemented, the whole cycle was reviewed once more to make sure all the solutions were matching the actual goals set. This was done by testing the theory against practice and further developing the solutions if the goals weren't met. The case study result analysis and documentation was done on this stage.

Conclusion stage consisted wrapping up the internal project as well as doing the result analysis and final conclusions. This stage also provided some future design cycle opportunities.

## 2 DATA CENTER ENVIRONMENT AND BUSINESS REQUIREMENTS

When planning or building a new data center, it is crucial to understand the current environment to achieve the best possible outcome. The following chapter defines the current data center platform to which the new modern data center was to be built.

### 2.1 Data center environment

Organization in question has operations in eight different countries including the Nordic countries, Baltics and Russia. Data center operations are concentrated in two main sites where most of the business-critical services are hosted. Local applications and requirements however demand the platform to be universal and to cover the local requirements as well. Based on the business requirements, the organization therefore has eighteen different data centers in total, all of which have been listed in figure 2.



FIGURE 2. Organizations data center sites

All the data centers are currently utilizing VMWare's virtualization platform. System hardware has been calculated to meet the local business requirements and all sites are using a harmonized hardware vendor, which in this case was IBM. Depending on the local infrastructure and organizations history, different network and storage configurations make the hardware platform sometimes very heterogeneous and therefore difficult to maintain. By using standardized platform vendor and hardware options, the data center design aims to be as universal as possible.

## 2.2 Data center business requirements

Organization operates on multiple different market fields such as food industry and restaurant services. Data center operations need to be able to provide operations in all countries as well as be traversable between different business units. This puts high requirements for the data center specialist when designing data centers that can meet all the business requirements. These business requirements vary based on the business application, but in general almost all essential applications require the data centers to be running 24 hours a day, 7 days a week, 365 days in a year. Summary of most widely used applications and their impact to data center operations has been gathered into the table 1. The key point that can be seen from the table is that the core services require data center to run continuously.

TABLE 1. Business service impact on data center

Service	General time of operations	Business impact	Data center impact
Office applications	Office hours Monday-Friday 07-18	Medium to low	Authentication services need to run 24/7/365
Collaboration tools	24/7/365 operations	Major to high	Authentication services need to run 24/7/365
Business critical applications	24/7/365 operations	Major	Data center operations need to run 24/7/365
Printing	24/7/365 operations	Major to low	Data center operations need to run 24/7/365
Reporting & forecasting	24/7/365 operations	Major to medium	Data center operations need to run 24/7/365
Non-critical business applications	Office hours Monday-Friday 07-18	High to low	Data center operations need to run during office hours
Web Applications	24/7/365 operations	High to low	Data center operations need to run 24/7/365
Citrix platform	24/7/365 operations	Major to low	Data center operations need to run 24/7/365
ERP	24/7/365 operations	Major to high	Data center operations need to run 24/7/365

As can be seen from the table 1, any sort of business essential or critical application immediately sets round the clock requirements for data center operations. To meet these requirements, the data center platform is required to be built upon high-availability platform, which is then backed up by working disaster recovery design. High-availability platform in this case has been solved by using VMWare's cluster technology, where two or more hosts work together to provide a functioning platform for virtual machines. The organization had identified a growing need for a standard disaster recovery, which currently had been loosely implemented on different business solutions.

The requirements for disaster recovery had been driven by the business after they were identified by the internal ICT personnel. Disaster recovery in plain terms for this organization meant keeping the business rolling, or bringing the business back online as fast as possible when a catastrophe occurs. Several business functions are completely crippled if the key components in data center environment are not working. Since the organization relies heavily on VMWare's virtualization, having this virtualization platform completely offline means that lot of the business functions will seize their operations until the platform has been brought back online. Securing the known key components is the main responsibility for the data center specialist, as well as keeping backups for those systems which may need to be recovered but are not immediately business critical when a failure occurs.

In such a multilayered environment, where business needs drastically differ between business units, a good documentation and communication methods play important role for the business continuity. The organization had started to implement critical incident and MIM processes to handle any possible error situations in a controlled manner. These processes follow the industry standards and MIM will be covered more in detail on a later chapter. The data center specialists are in constant communication with the business key users to keep the application platform synchronized

with the current development of the ICT field. It has also been recognized that business processes for this organization are not usually able to follow the speed of the current technological development. This means the data center specialist needs to be able to find long-term solutions that are scalable within the data center platform. This results that the environment should be able to support a wide variety of technological solutions, which come with vastly different lifespans.

### 3 MODERN DATA CENTER

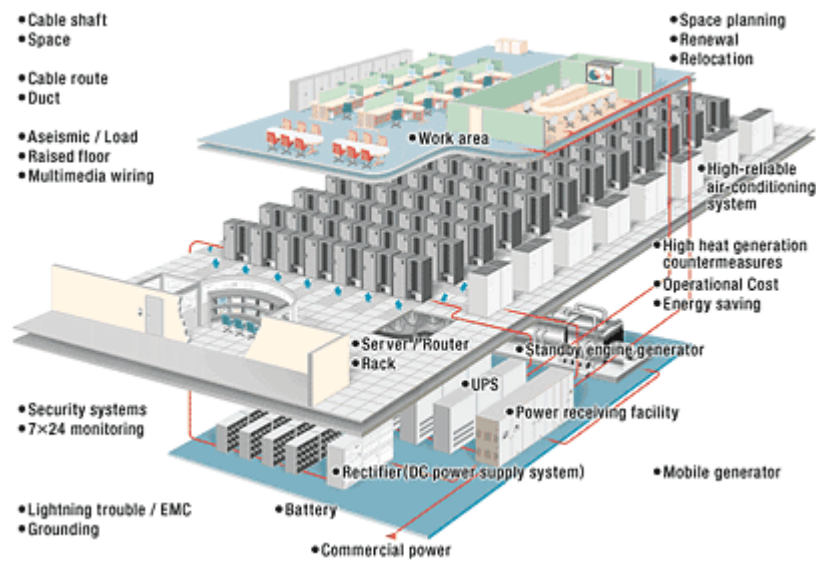


FIGURE 3. Example of a data center layout (NTT Facilities 2017)

Standard for data center infrastructure was first introduced in TIA-942. Ever since then modern data center designs have received several more detailed specifications, because the TIA-942 is mainly focusing on telecom infrastructure standard (Telecommunications Industry Association 2012). An example of a large modern data center can be seen in figure 3, which includes things such as space management, security, hardware and cabling.

Data centers are presented from a tier perspective by all major industry standards, such as ANSI/TIA-942-A, ANSI/BICSI, EN 50600-x and their commercial counterpart UPTIME INSTITUTE (Telecommunications Industry Association 2012). There is only a slight variation in specifications between different tiers, as can be seen on table 2. Mostly the differences are in the way how the redundancy has been defined in each tier.



TABLE 2. Data center tiers

	TIER 1 - Basic data center	TIER 2 - Redundant Components	TIER 3 - Concurrently Maintainable	TIER 4 - Fault Tolerance
ANSI/TIA-942-A	No redundancy	Single distribution path with redundancy	Multiple distribution paths with only one active	Multiple active distribution paths
UPTIME INSTITUTE	Data center provides dedicated site infrastructure to support information technology beyond an office setting	Facilities include redundant critical power and cooling components to provide select maintenance opportunities and an increased margin of safety against IT process disruptions that would result from site infrastructure equipment failures.	Data center requires no shutdowns for equipment replacement and maintenance.	Adding the concept of Fault Tolerance to the site infrastructure topology.
EN 506000-X	No specific requirements	Single-path (no redundancy of components)	Single-path (resilience provided by redundancy of components)	Multi-path (resilience provided by redundancy of systems). Allows maintenance during operation
ANSI/BICSI 002-2014	Single Path	Redundant components	Concurrent Maintainability	Fault Tolerant

Commonly anything beyond normal office setting, that is hosting something for an organization, is considered a data center. As the organizations size grows, the data center is usually located on a specific room designed for data center operations. This room should provide facility functions such as redundant power, cooling and access control. The Information Technology (IT) equipment should be using multiple-paths for component redundancy wherever it is possible. When the requirements for data center operations increase, fault-tolerance and disaster recovery are things that need to be introduced as variables, which then leads in the escalation of the data center tier. (Telecommunications Industry Association 2012; Diminico 2006.)

### 3.1 Data center standard comparison

According to a forecast created by Research and Markets, the Western Europe will see grow of CAGR (Compound Annual Growth Rate) of 8.47% during 2014-2019 for data center construction market. This means as new data centers are being built the need for standardization grows. (Researchandmarkets 2016.)

TIA-942-A and ANSI/BICSI 002 have first emerged in United States and as their counterpart, the EN 50600-x has been created in Europe.

Recommendation on which standard the organization should choose, is solely based on the actual location(s) of the data center. Companies that want to follow the latest standardization currently available in Europe or United States, the EN 50600-x is the one to choose. In table 3, are listed the differences between the currently available standard specifications in Europe and United States. The table 3 shows how EN50600-x covers energy efficiency enablement and management & operation, while other standards do not have cover them fully. (Commscope 2015.)

TABLE 3. EN50600-x vs. other design standards (Commscope 2015)

	50600-x	TIA-942-A	ANSI/BICSI 002	Commercial Assessors
Scope	All DC facilities & Infrastructures	Cabling only	All DC facilities & Infrastructures	Mainly Power & Environmental Control
European Standard	✓	✗	✗	✗
Regional Application	Europe/Internationally applicable by using ISO/IEC standards as references	United States	United States	International
Energy Efficiency Enablement	✓	✗	✗	✗
Management & Operation	✓	✗	✗	?
Inclusion of global KPIs (ISO/IEC 30134-x)	✓	✗	✗	?
Commercially Neutral	✓	✓	✓	✗
Independent Assessment	✓	✓ (Cabling Only)	?	✗
Business Approach (design vs cost)	✓	✗	✗	✓

Standardization provides a good basis when planning for data center construction, but sometimes different standards are in contradiction with one another. Rule of thumb in following the standards is to go with the most stringent requirements while following industry accepted practises, without forgetting the location of the actual data center. (Lam 2016.)

### 3.2 Site selection

When choosing the best location for a data center, there are multiple things to consider. Will the data center be functioning as a primary site, secondary site or perhaps specifically made for disaster recovery. Based on the requirements, it is possible to draw cost evaluation for utility services such as power and electrical, communications, water and sanitary as well as natural gas and other fuels. (Invest in Finland 2016.)

In Finland the risk for most natural hazards is low and regarding this aspect Data Center Risk Index lists Finland as one of the safest places to build a data center. However Finnish power grid is also one of the most affected in Europe by the harsh winter and there has been criticism on the power grid reliability based on this. There is also always the requirement to be prepared for manmade hazards. Proximity to an existing or redundant data center and skilled labour always plays a factor when deciding on the location. Having long distances may hinder the possibility to recover swiftly from a possible hazard. (Invest in Finland 2016; IEEE 2017.)

Finland serves as a node point between East and West, providing very good global data connections. While data connections are a necessity for a data center, having a good public road access is also a thing, which plays a factor in larger data centers. (Invest in Finland 2016.)

In addition to standardization, country regulations may also be a factor, which data centers must abide. Having a pre-set of rules and regulations also requires security and emergency services in the background, which

need to be considered when building a new data center (European Commission 2017).

### 3.3 Space planning

As well as good location, a good physical space is one of the corner stones of a new data center. Well-equipped data center has enough space to meet current needs as well as incorporate valid options for expansion. Managing physical space becomes easier with modular design, so each rack space, cable route and aisle should be thought with this design in mind. Moving, adding or removing these modular components allows the data center to shape into a form, which serves the current needs in a best possible way. (Rasmussen & Torell 2015.)

Design parameters are defined by the factor is the data data center to be placed in pre-existing or in a totally new space. Pre-existing spaces sometimes define most of the outer connections for airflow, electricity and network cabling as well as possible existing fire safety.

Access control and other building maintenance related facts, which directly effect on the space planning efficiency are also befined by pre-existing spaces. While these things might limit the choices how the data center space layout can be done, they also provide clear guidelines as to what can be done. Building a totally new data center in a new location allows the planning to be done from ground up, resulting in a situation which most likely much better reflects the official guidelines for new data centers. However, building a new space requires a lot more planning work and requires a bigger design team to achieve the best possible outcome. (Rasmussen & Torell 2015.)

### 3.3.1 Rack space

Ensuring you will get right amount of rack space requires data center administrator to estimate the necessary rack space for the equipment and cables. Generally, it is good to not fully stack a rack if there is a possibility to leave room for new equipment and/or installation space for actual installation tasks. Heaviest estimated rack weight needs to be calculated when a floating floor is used. Having too much load on a single spot may cause structural damages, which are very hard to fix when the data center is fully operational. Calculating required equipment and doing a sketch on where to install everything and how are different hardware equipment interconnected, gives the best possible outcome when the actual hardware installation is done. (Rasmussen & Torell 2015.)

Aisles need to be kept enough apart so that full length hardware can be installed and maintained from both sides of the rack. If the data center space allows for extended space between racks, it is always a good idea to leave it available, since it allows personnel to bring heavier hardware components nearer to the racks for installation. (Rasmussen & Torell 2015.)

### 3.3.2 Electricity

Each data center rack requires two minimum components: power and network cabling. Power distribution to each rack should be calculated with the heaviest possible load based on the manufacturer's notified specifications for IT equipment. Most common IT equipment requires two power plugs for redundancy. This means the racks should be equipped with enough rack mounted power distribution units (PDUs) to serve the fully stacked rack. Each PDU should have its own power source, so one faulty equipment does not cause any power problems to the connected devices. Calculating necessary power cabling is based on the estimated load, amount of PDUs and the amount of racks. (Hu 2017.)

Incoming power to the data center needs to be continuous and uninterrupted. Achieving this means multiple power routes to the data center with their individual power sources. Basic landline power source needs to have its own backup. Maintenance breaks and accidental power losses from primary electrical power system requires alternative power source such as a battery operated Uninterrupted Power System (UPS) or a diesel generator to keep the data center operational. The capacity for UPS should be enough to support data center for few hours and a diesel generator is usually used to keep the data center running after that until primary electrical system has been mended. In large data centers, the amount of diesel reserves also need to be calculated so that the power distribution does not suffer from the lack of fuel. (Ryan et al. 2009.)

### 3.3.3 Network cabling

Network cables in data centers are serving as the lifeline of every data bit going in or out. There are two layers of data cabling: cabling to and from the data center and the cabling inside the data center. The cabling which interconnects data center with outside network should be redundant. At least two distribution routes for cabling must exist to ensure stable and fault-tolerant data connections. Outside cable routes are usually hard to manage, so while building the data center it is always a good idea to reserve extra cabling that is not immediately taken into use. In most cases the cables themselves usually cost less than the cost for actual installation work, so as a cost saving for future it is good to over capacitate the network cabling requirements. (Brocade Communications Systems 2007; Dumitru 2017.)

Cabling inside data center can be achieved using multiple different technologies. As a rule of thumb, the data center cabling should be as universal as possible. Interconnected cabling between racks ensures that no long individual patch cabling is needed. Having patch panels into which you can connect the devices on each rack is a minimum requirement for a

modern data center. The type of patch panel depends on the devices installed into the racks. Most commonly single-mode fiber, multi-mode fiber and CAT6-cabling are used for device connections. Ensuring there is enough these ports should provide a solid base for device interconnectivity. There are commercial products available, which provide multiple panel connections for devices, while the cable between two panels is very thin compared to running all the cables individually between the racks. These kinds of solutions allow more clean-cut finish to the data center cabling, but are financially more expensive. (Belden Inc. 2009.) One example of a robust future-proof data center internal cabling design can be seen in figure 4. The figure displays a way to connect all racks with each other using both copper and fiber cabling.

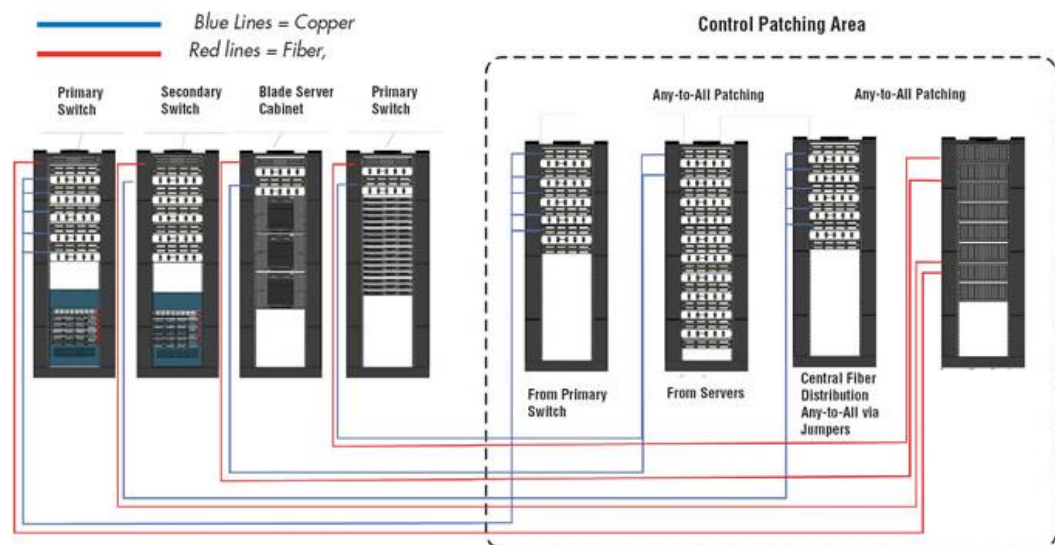


FIGURE 4. Example of Any-to-All structured cabling (Siemon 2009)

### 3.3.4 Temperature & cooling

All the hardware equipment in the data center is going to create a lot of heat. Keeping the data center cool is crucial to keep equipment up and running. Designing airflow in racks gives you few options: front-to-back, front-to-top and front-to-top-and-rear. The best possible airflow depends on which hardware is installed in the racks. The main goal is to keep any heat pockets from forming within the rack cabinets, while cold air freely flows into every single device. Too high operating temperature causes shorter equipment lifetimes and possible even hardware malfunction. Recommended operating temperature for data centers varies between values from 18-27 degrees Celsius, while 22 degrees Celsius is the most recommended value. In addition to temperature, relative humidity recommendation is to be kept between 20-80%. (Cisco 2017.)

Aiming for duplicated cooling devices should always be a goal, since there is always the possibility for a hardware failure. Future cooling hardware changes are also easier to achieve when the data center operations do not need to be stopped for device maintenance. For smaller data centers a pair of an air source heat pump (ASHP) should be adequate, while bigger data centers require dedicated large cooling devices. Figure 5 is psychrometric chart providing an illustration on how thermal and moisture levels affect one another and how cooling can be planned more effectively. The figure displays how connecting the dry bulb temperature (air temperature) and wet bulb temperature (adiabatic saturation temperature) in a psychrometric diagram gives the state of the humid air. (ASHRAE Technical Committee 2011.)



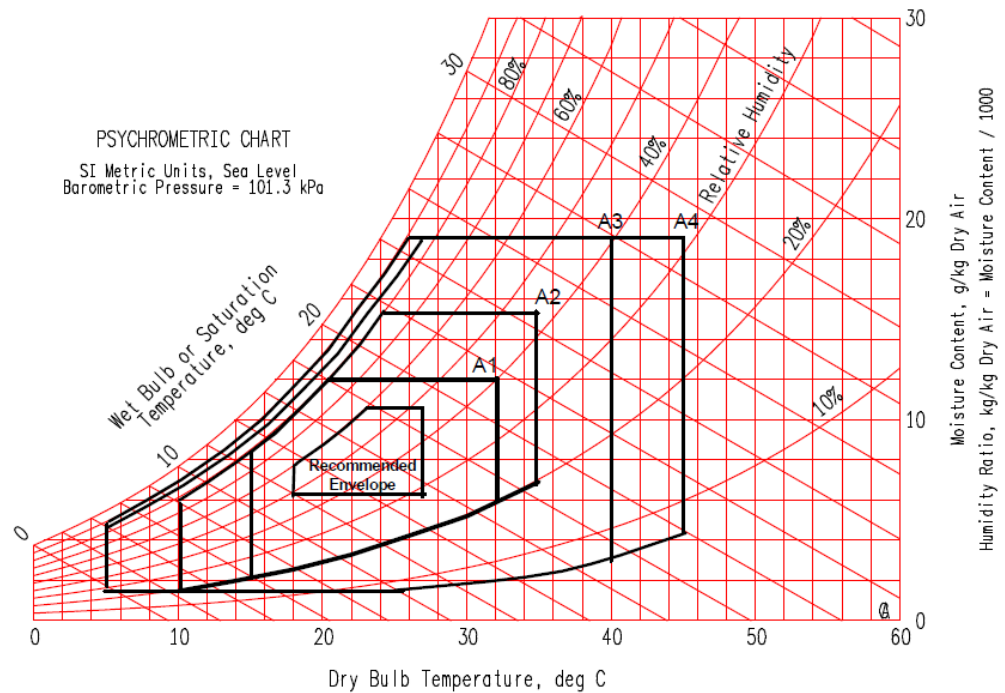


FIGURE 5. ASHRAE Environmental Classes for Data Centers (ASHRAE Technical Committee 2011)

### 3.3.5 Fire suppression

Keeping a data center cool also means keeping it from not catching fire. There are multiple fire suppression systems for data centers, and currently they all usually fall into two categories: clean agent systems and inert gas systems. Clean agent systems are commonly based on halocarbons and they work by removing heat from the fire while inert gas systems deprive oxygen causing the fire to stop burning. (Lo Bosco 2011.) Figure 6 shows a fire suppression system using a gas based product and how each part of the system is connected to the control panel.



### 3.3.6 Lighting

To avoid any hazardous situation in data centers, adequate lighting should be installed to cover all necessary areas. Light emitting diode (LED) lighting is typically recommended over fluorescent lighting because they consume less electricity, generate less heat and they are dimmable. Generally lighting in data centers consists 3-5% of the overall energy load, so lighting choices should not be overlooked. (PennWell Corporation 2014)

When designing lighting it is good to estimate when and how the lights are turned on and are they turned on to the whole data center or just a section of it. Position of the lights need to be decided depending how the racks are arranged and are there overhead cabling routes that might cause dark spots within the data center. There are also rack lights available on the market, which provide dedicated light within a certain rack to cover those hard to reach places with general lighting. (Commscope 2014.)

### 3.3.7 Supporting spaces

Supporting spaces for data center consist areas such as loading dock and storage. Well accessible loading dock ensures a route for heavy hardware equipment to be moved to and from the data center. Most IT hardware is so heavy, that they cannot be lifted safely by a single individual and carrying equipment for extended distances causes a risk of injury to the personnel or possible damage to the hardware. (Clark 2014.)

Accessible storage space in the near vicinity of the data center ensures that the data center administrators have always a place to store necessary installation hardware close-by, while keeping the actual data center clean. Many of the data center certifications as well as fire safety rules indicate that unnecessary hardware or installation material should not be stored within the actual data center. Storage place that is not close to the actual

data center may cause unnecessary personnel costs or delays in installations. (Clark 2014.)

### 3.3.8 Access control

Security in data centers can be done on a very detailed level. Most data centers do not need to plan for extreme cases such as bomb detection, but all data centers need to have some form of access control. Limiting the amount of physical access doors to the data center minimalizes also the physical access control. Door access for data centers should be handled in a way that the system can identify the individual entering the data center and log the information in a secure location. Figure 7 portrays a user entering a data center using a keycard identification. (Scalet 2015.)



FIGURE 7. Identifying individual entering a data center (Pater 2015)

In addition to electrical access control, a common requirement is that security cameras need to be operational so that all activities within a data center are also logged. Motion-sensor cameras and low-light cameras are recommended and saving the digital footage off-site further increases security since it can not be tampered with. (Scalet 2015.)

Access inside the data center should also be managed by locking each rack door and providing individual access to the racks for selected individuals. Also as a part of physical security a periodical check-up on agreed safety standards should be conducted to ensure any possible security breaches. Data center administrators are encouraged to out-source access control to minimize possible abuse of access permissions. The storage requirements for a data center heavily depend on the size of the data center and the hardware choices made. (Scalet 2015.)

### 3.4 Architectural issues

Choosing the correct architectural design can be very challenging. When aiming for high-availability, a good design plays a key-role. Finding the best solutions means end-to-end process thinking with an eye for the future.

#### 3.4.1 Reliability

Reliability comes without any downtime, so planning for a data center that minimizes the risk of downtime saves organizations a lot of money. Even the best-in-class organizations experience downtime, so companies should prepare to minimize the time length of these downtimes (Bell 2005).

Components and systems have a certain reliability rate, so instead of focusing on best possible reliability, organizations should thrive for best possible availability. Customers nowadays are always asking for always-on availability and they are not used to any downtimes. Having even a short unplanned downtime may cause damage to the organizations image or credibility and directly or indirectly affect negatively on the revenue. (Bell 2005.)

Monitoring and control capabilities have vastly increased within the last decade. Organizations aiming for best availability need to proactively monitor any changes within their systems and predict any possible errors within the data center (ECD Solutions 2017).

There will always be time when repairs or hardware changes must be done within the data center. Hardware platform can be built in a way that it is inspected periodically limiting the chance for a possible hardware failure. Another possibility is to design the hardware environment so that it does not matter if a component fails since it can be replaced whenever. First option requires more personnel to monitor the system and do the inspections, while the second one requires more investment in hardware side. (Bell 2005.)

### 3.4.2 Availability

Round the clock operations for whole year needs vast amount of planning and testing. Every single component needs to be fault redundant or the component must be part of a high-availability solution in some way. Component health and complex system configurations require administrators to continuously check their environment health to ensure that in-case of an error, these costly high-availability or disaster recovery systems do what they are designed for. Failure to overlook these things might cause companies to lose revenue when a system failure occurs. (Schulz 2009; Vaidyanathan et al. 2004.)

True availability is only achieved when every piece of hardware and software come together perfectly. This however is not possible, since there are always unknown variables in play. To get closer to providing true availability, disaster recovery technologies need to be implemented on a level that allows the systems to move between multiple data centers in completely different physical locations. (Schulz 2009; Vaidyanathan et al. 2004.)

High availability control, advanced data collection, advanced analytics, critical alarm response and integration of all systems create a combination for a highly reliable data center. Fully redundant systems with working DR site helps the organizations keep their business up and running continuously, thus providing good availability. (Schulz 2009; Vaidyanathan et al. 2004.) Disaster recovery is covered in detail later in chapter 4.

### 3.4.3 Labeling

Easily identifiable hardware devices and racks within data centers minimizes time spent looking for certain devices when they are not reachable over network. It also minimizes risk when performing maintenance breaks which include changes in the current infrastructure. Labelling should include at least racks, cable shelves and devices, which are found within a data center. (Panduit 2014; Jew 2016.)

As well as having the labels on right places, it is also as critical to have a clear naming standard for these labels. Good labels usually use acronyms along with some form of alphabetical numbering system. Depending on the scale of the data center, it might also be wise to have sections from within certain labels are found and these sections written into a map for the data center. (Panduit 2014; Jew 2016.)

## 4 DISASTER RECOVER AND MAJOR INCIDENT MANAGEMENT

Defining disaster recovery requires the definition for disaster recovery site. “A disaster recovery site is a facility an organization can use to recover and restore its technology infrastructure and operations when its primary data center becomes unavailable.” (Rouse 2015.)

Disaster recovery in a nutshell is data recovery and service continuity after a failure or a disaster. With disaster recovery sites companies aim to minimize the impact of disasters. To fully utilize a disaster recovery site, the organizations need to establish business impact analysis on their environment along with risk analysis. Based on these two, organizations can produce a working disaster recovery plan. Understanding the impact, identifying critical assets and restoring functions after a disaster, is the main goal when planning for disaster recovery. (Cisco Systems, Inc. 2006.)

### 4.1 Disaster recovery facilities

While organizations may have very effective data redundancy in their onsite data center, they often overlook the requirement for offsite data storage. Disaster recovery is a situation which companies should thrive to avoid. To achieve this there should be redundancy created for heating, ventilation and air conditioning (HVAC), physical connectivity paths and devices as well as for power and storage. On the software layer, technologies such as mirroring and redundant array of independent disks (RAID) are things which can further increase redundancy and prevent the need for a disaster recovery. On-site data center redundancy is a way to provide fast recovery from any hardware or software error without the need for disaster recovery. (Bahan 2003; Wold 2013.)

Disaster recovery can be built in various ways depending what are the business needs. Data center duplication is one of the most robust ways of creating disaster recovery, since the aim is that you can lose a whole site without affecting any of the business processes. If data center duplication



is not a possibility, organizations can build their own data center specifically for disaster recovery purposes with minimal required hardware to keep the business rolling, or they may opt for colocation facility. Colocation facility is a data center from which services are provided for rental to retail customers. (Bahan 2003; Wold 2013.)

#### 4.2 Disaster recovery plan

Disaster recovery plan (DRP) is a part of Business continuity plan (BCP). The business continuity plan consists the following component:

- Business Resumption Plan
- Occupant Emergency Plan
- Incident Management Plan
- Continuity of Operations Plan
- Disaster Recovery Plan

Disaster recovery itself is not able to provide full business continuity, but it is a key element when ensuring it.

Disaster recovery is a documented process, which defines how the organization should act in a sudden, unplanned catastrophic event which prevents the organization to carry on its critical or mission-critical processes. Table 4 can be used a way to classify which applications and/or systems should be handled as a priority one in case of a disaster recovery. (Martin 2002; Wold 2013.)

TABLE 4. Classification of Application/System (Bahan 2003)

Classification		Description
1	Mission Critical	Mission Critical to accomplishing the mission of the organization Can be performed only by computers No alternative manual processing capability exists Must be restored within 36 hours
2	Critical	Critical in accomplishing the work of the organization Primarily performed by computers Can be performed manually for a limited time period Must be restored starting at 36 hours and within 5 days
3	Essential	Essential in completing the work of the organization Performed by computers Can be performed manually for an extended time period Can be restored as early as 5 days, however it can take longer
4	Non-Critical	Non-Critical to accomplishing the mission of the organization Can be delayed until damaged site is restored and/or a new computer system is purchased Can be performed manually

The DRP is an ICT focused plan, and its purpose is to help organizations to return to normal operations as soon as possible. Key objectives for returning to normal operations are Recovery Time Objective (RTO) and Recovery Point Objective (RPO). RTO defines how long can recovery take and RPO defines how much data can be lost due to the recovery process. To find these key objectives a Business Impact Analysis (BIA) needs to be performed. BIA defines the criticality level of the system or application. The decision for the RTO and RPO times must come from the upper management, since they are the ones to decide acceptable amount of information loss. Usually these values are driven by the amount of lost revenue when disaster recovery process needs to run its course. (Martin 2002; Wold 2013.)

As previously mentioned, disaster recovery plan is just one step in the overall ICT DR planning process. The whole process itself covers the following seven things:

1. Business Contingency Planning Policy and Business Process Priorities
2. Risk Assessment
3. Business Impact Analysis (BIA)
4. Business Continuity and Recovery Strategies
5. Business Continuity Plans
6. Awareness, testing, and training of the DRP
7. Disaster Recovery Plan maintenance and exercise

The main task for DRP is to minimize business impact with an acceptable level of risk accepted by the senior management. From these seven steps, the BIA is the most time consuming and most expensive one. Calculating return on investment (ROI) is usually the way to get management involved to conduct analysis and therefore justify the planning for continuity and recovery strategies from a technical point of view. The whole background analysis and technical solutions are then tied to the actual business processes by developing strategies for business continuity. The whole process requires training and awareness from the whole organization level as well as making sure the DRP plan evolves along with the business. Periodical testing for all the previously set requirements is the only way to ensure business continuity. (Martin 2002; Wold 2013.)

#### 4.2.1 Using the disaster recovery plan

After business process recovery time objectives and recovery point objectives have been identified, these business components need to be tied to their respective ICT systems and applications. ICT solutions then need to be designed in a way which supports the business needs. Business process may depend on single or multiple applications, which therefore need to be also covered with similar classifications. (Martin 2002; Wold 2013.)

In today's converged data center solutions many applications share the same platform. The system recovery time (SRT) needs to be set according to the shortest recovery time objective of an application, which is hosted on top of that platform. Also identifying the personnel whom maintain these systems is required for the SRT to be applicable. All hardware components which are part of a host system, which then support the business application, need to be identified and be included to get a valid system recovery time. (Martin 2002; Wold 2013.)

Copying verified data to an offsite storage facility should be included in normal operations for any data center solution. Data can be either transmitted through a Wide Area Network (WAN) connection or by using physically removable media such as tape. The main goal is to have the necessary data defined by the recovery point objective, shipped to an off-site location and to be ready to be restored in a timeframe that is defined in the recovery time objective. (Martin 2002; Wold 2013.)

Having the right people for the right job is a key element for any disaster recovery situation. Organizations should have clear chain of command during disaster recovery situations as well as the necessary personnel on-site and agreement in place with 3<sup>rd</sup> party vendors to support in case of an emergency. Key personnel should take immediate action when disaster recovery plan needs to be set in motion. All personnel should be trained to

operate correctly in a DR situation to minimize the damage and restore normal operations as quickly as possible. Understanding of the disaster recovery processes throughout the organization ensures that the key personnel can focus on their tasks if a DR situation should present itself. (Martin 2002; Wold 2013.)

#### 4.2.2 Testing the disaster recovery plan

For any disaster recovery to succeed, there is a need to thoroughly test and evaluate the written DR plan. Clear and documented test procedure should be written so that the organizations can make sure that they have a working DR plan. After every testing, the test plan should be reviewed and updated if necessary. (Martin 2002.)

DR testing is to demonstrate the organizations ability to recover, while identifying areas that need further development. All facilities and procedures regarding backups should be reviewed for operations and organizations should make sure that their personnel have had proper training to carry out any DR situation. Testing should be done in a way which causes minimum business impact (Martin 2002; Wold 2013.)

By annually simulating the actual DR situation, organizations can make sure that their business-critical services are able to resume normal operations. Organizations may also aim to test a subset of the DR plan, to validate more frequently or to make sure that a change within that subset has not caused any deviations onto the DR plan. Different types of tests can be listed in the following way: Checklist tests, Simulation tests, Parallel tests and full interruption tests (Martin 2002; Wold 2013.)

After a DR plan is written and fully tested, the top management should review the results and approve the plan or make necessary corrections to it. Consistency planning is always the top management's responsibility. (Wold 2013.)

## 4.3 Major Incident Management

### 4.3.1 Major Incident definition

Major Incident Management is above organizations normal incident process routines. Major Incident Management is usually described as an incident that fits the major incident procedure or has or may have impact on critical services and/or systems defined by the organization major incident procedure. It may also be an incident with impacts organization in a way that has negative effect on reputation, legal compliance, regulation or security. (Ucisa 2016.)

Major incident management is all about handling situations that are out from the normal operating procedures. Well documented and trained MIM process helps companies revert to normal operations in a swift manner. Usually MIM refers to the organizations existing SLA (service-level agreement) agreements about the necessary recovery point objective and recovery time objective. (England 2014; Nolting 2013).

### 4.3.2 Major Incident standards and best practises

Organizations preparing for MIM usually turn into looking guidance from ITIL (Information Technology Infrastructure Library) documentation for the known best practises. For those organization looking for certification or their MIM process to be audited, they should consider using the ISO/IEC 20000 standard. This standard is split into two parts ISO/IEC 20000-1 explaining what needs to be done and ISO/IEC 20000-2 telling how it should be done in detail. There are also additional six parts for the ISO/IEC 20000 standard which cover following areas: scope definition, scope applicability, process reference model, implementation plan, application to the cloud, concepts, terminology and guidance for framework relationship. The approach used depends is the organization aiming for ITIL implementation or the ISO/IEC 20000 certification. (20000 Academy 2016; Valentic 2016.)

There are differences between the relationship of ISO/IEC 20000 and ITIL as can be seen in figure 8. ISO/IEC 20000 is aimed to be applicable no matter what the size of the organization is, while ITIL has recommendations depending the size of the organization. ITIL also targets individual processes, while ISO/IEC 20000 aims for continuous improvement. Regarding process comparison there are quite a lot of differences between these two. The following processes are at least partially different between the two approaches: business relationship management, supplier management, reporting, budgeting, accounting, information security, capacity management and asset management. (20000 Academy 2016; Valentic 2016.)

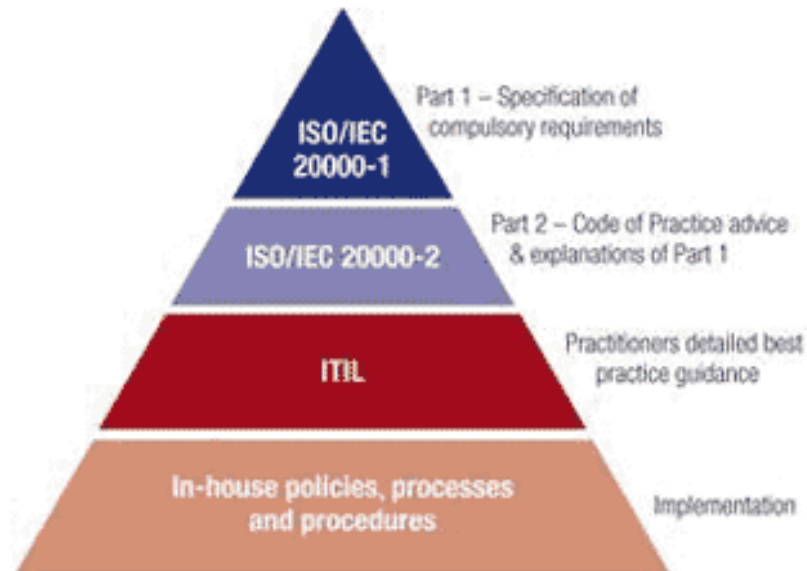


FIGURE 8. Relationship between ISO/IEC 20000 and ITIL (Dugmore & Holt 2016)

### 4.3.3 Major Incident process

Core objectives for MIM process are:

- Efficient resolution of incidents that have a major impact on business and critical business processes
- Ensure quality and quantity of communication during major incidents
- Ensure sufficient resources for major incident resolution
- Prevent similar incidents from reoccurring via a systematic post incident review

To ensure these objectives are met, the organization needs a correct workflow during MIM process. An example of such a workflow can be seen in figure 9. As the workflow demonstrates throughout the process, communication is the key for any successful handling of a major incident. (Enisa 2010.)



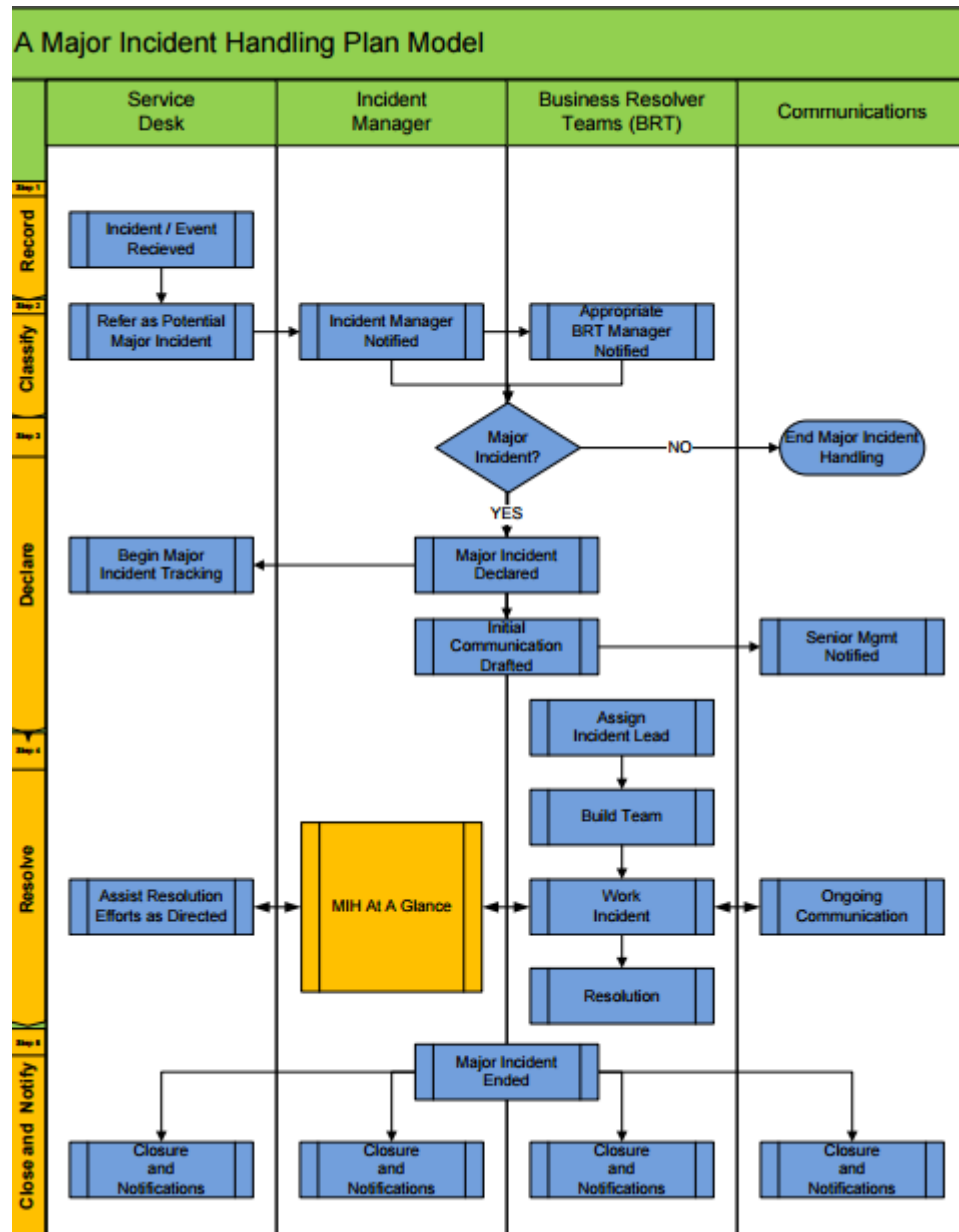


FIGURE 9. Example Major Incident Workflow (BraunsBlog 2012)

For MIM management to work, it also needs a suitable major incident team. This major incident team consists of service desk manager, incident manager, major incident manager, problem manager and other members. The main goal is to have a team who can swiftly and accurately tackle the incident in question, while maintaining good communications with the customers. Major incident team is also responsible for the root cause analysis after the incident has been solved. (ITIL Service Management 2011.)

## 5 CASE STUDY

### 5.1 Research approach

This case study uses predictive research method to estimate the possible requirements for the new data center. Predictive research methodology cycle can be seen in figure 10. Predictive research was chosen, because the basic environmental data was available for the current platform, but with the pre-existing complex environment, it was unknown how the end-result will turn out. Aim for the predictive research is to take the data you have, to predict the data you do not have. In this case study, the basic platform data was available, but there was not any concrete way to calculate how much resources were needed to be reserved to meet the end-result. (Bertolucci 2013; The Design-Based Research Collective 2002.)

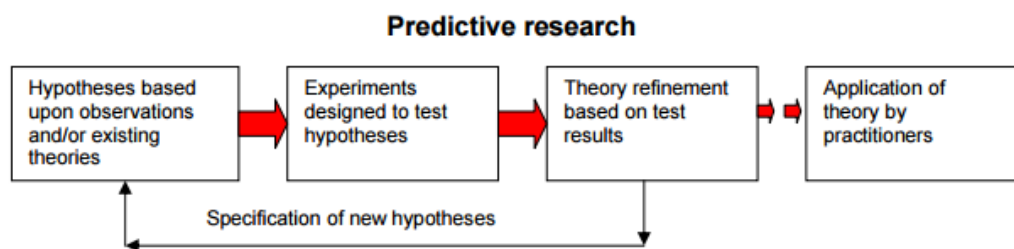


FIGURE 10. Predictive research method (Amiel & Reeves 2008)

## 5.2 Data collection

The case study is limited to the main data center, which is in Southern Finland, but it aims to serve as a basic platform that can be expanded to meet the requirements for all sites within the organization. Whole platform consists of 39 VMWare hosts on 18 sites, hosting 621 virtual machines in total. The list of virtual machines and hosts per site can be seen in figure 11. Wan connections on sites vary from 4Mb – 1Gb.



















Name	Hosts	Virtual Machines
 Eskilstuna	1	7
 Helsinki	1	1
 Karkkila	1	2
 Kaunas	1	3
 Lövvånger	1	7
 Lahti	2	3
 Lappeenranta	4	24
 Lidköping	2	12
 Lund	1	5
 Moscow	1	9
 Odense	1	4
 Ogre	1	3
 Oulu	1	5
 St.Petersburg	4	65
 Stockholm	1	9
 Tallinna	1	2
 Umeå	1	4
 Vantaa	15	456

FIGURE 11. Sites, hosts and virtual machines

Case study is focused on sites Vantaa and Lahti and disaster recovery environment is limited to only certain virtual machines, which have been identified as most business critical.

Data gathering from virtual center was done by RVTools. Based on this data, an estimation for disaster recovery capacity planning was made. An example of such listing can be seen in table 5, which includes information such as virtual machine name, cpu, memory & network configuration. The virtual machine names have been altered to shield organizations privacy.

TABLE 5. Example of virtual machine requirements on disaster recovery site

VM	CPUs	Memory	NICs	Network #1	In Use MB	Datacenter	OS
DC1	2	4 096	1	LAH-SRV-3	101 864	Vantaa	Microsoft Windows Server 2008 R2 (64-bit)
DC2	4	4 096	1	MET-INF-752	132 618	Vantaa	Microsoft Windows Server 2008 R2 (64-bit)
PROD1	2	4 096	1	Server VLAN 3	63 522	Lahti	Microsoft Windows Server 2008 R2 (64-bit)
PROD2	4	18 432	1	MET-SRV-753	192 956	Vantaa	Microsoft Windows Server 2008 R2 (64-bit)
INTEGRATION1	2	2 048	1	MET-DMZ-1-769	37 099	Vantaa	SUSE Linux Enterprise 11 (64-bit)
PROD2	1	2 048	1	MET-SRV-753	24 231	Vantaa	Microsoft Windows Server 2008 R2 (64-bit)
PRINT1	2	4 096	1	MET-SRV-753	25 289	Vantaa	Microsoft Windows Server 2008 R2 (64-bit)
VIRTUALCENTER	4	16 384	1	MET-SRV-753	116 878	Vantaa	Microsoft Windows Server 2008 R2 (64-bit)
POWERSHELL	2	4 096	1	MET-SRV-753	35 389	Vantaa	Microsoft Windows Server 2008 R2 (64-bit)
<b>TOTAL</b>	<b>23</b>	<b>59 392</b>	<b>9</b>		<b>729 846</b>		

Estimation for the data requirements were made with VeeAMs restore point simulator. In figure 12 there is an example of this restore point simulator based on the previously calculated values in table 5. This example is made with incremental backups that are built weekly into a full back using synthetic full backup technology, while keeping seven possible restore points on the disk. This weekly virtual machine backup schedule requires total of 1.6Tb of storage. This means that data compression and deduplication technologies can save up to 60% of disk space in the example given, but as VeeAM points out in their documentation, there are no guarantees and the actual values can only be seen in the live environment. More details about VeeAMs backup tool can be found from later chapter 5.5, Disaster recovery.

### Configuration

Style	<input type="text" value="Incremental"/>	<input type="button" value="⌵"/>
Used Size GB	<input type="text" value="730"/>	<input type="button" value="⌵"/>
Retention Points	<input type="text" value="7"/>	<input type="button" value="⌵"/>
Change Rate	<input type="text" value="10% Conservative"/>	<input type="button" value="⌵"/>
Data left after reduction	<input type="text" value="50% (100GB &gt; 50GB) 2x Conservative"/>	<input type="button" value="⌵"/>
Interval	<input type="text" value="Daily"/>	<input type="button" value="⌵"/>
Time Growth Simulation <input checked="" type="checkbox"/>	<input type="text" value="1 Year"/> <input type="text" value="10%"/>	<input type="button" value="⌵"/>

### Incremental Specific

Synthetic  MO  TU  WE  TH  FR  SA  SU

Active Full Weekly  MO  TU  WE  TH  FR  SA  SU

Active Full Monthly  Jan  Feb  Mar  Apr  May  Jun  
 Jul  Aug  Sep  Oct  Nov  Dec

### Run

Manual Run  Export  Canvas (experimental)

### Result

Retention		File	Size	Modify Date	Point Date
13 (7)		full.vbk	<a href="#">399.83 GB</a>	2017-11-04 Sa 22	2017-11-04 Sa 22
12 (7)		incremental.vib	<a href="#">39.99 GB</a>	2017-11-05 Su 22	2017-11-05 Su 22
11 (7)		incremental.vib	<a href="#">40 GB</a>	2017-11-06 Mo 22	2017-11-06 Mo 22
10 (7)		incremental.vib	<a href="#">40.01 GB</a>	2017-11-07 Tu 22	2017-11-07 Tu 22
9 (7)		incremental.vib	<a href="#">40.02 GB</a>	2017-11-08 We 22	2017-11-08 We 22
8 (7)		incremental.vib	<a href="#">40.03 GB</a>	2017-11-09 Th 22	2017-11-09 Th 22
7		incremental.vib	<a href="#">40.05 GB</a>	2017-11-10 Fr 22	2017-11-10 Fr 22
6		full.vbk	<a href="#">400.56 GB</a>	2017-11-11 Sa 22	2017-11-11 Sa 22
5		incremental.vib	<a href="#">40.07 GB</a>	2017-11-12 Su 22	2017-11-12 Su 22
4		incremental.vib	<a href="#">40.08 GB</a>	2017-11-13 Mo 22	2017-11-13 Mo 22
3		incremental.vib	<a href="#">40.09 GB</a>	2017-11-14 Tu 22	2017-11-14 Tu 22
2		incremental.vib	<a href="#">40.1 GB</a>	2017-11-15 We 22	2017-11-15 We 22
1		incremental.vib	<a href="#">40.11 GB</a>	2017-11-16 Th 22	2017-11-16 Th 22
			1240.93 GB		
			Work Space		
			<a href="#">+421.13 GB</a>		
			<hr/>		
			1662.07 GB		

FIGURE 12. VeeAM restore point simulator with weekly synthetic full backups

## 5.3 Background and design

### 5.3.1 Background

Organization in question was looking for a way to deal with their main data center site being offline or unavailable. To ensure business continuity, a cost effective technical solution was needed for business-critical applications.

Organization had decided to use one of their secondary sites instead of the currently available cloud solutions to minimize the costs and to avoid purchasing a dedicated network line for the cloud service provider. The goal was to design and build a new disaster recovery data center that would also serve as a local on-site data center for local requirements.

Building a modern data center requires extensive planning. To achieve the best possible outcome, the data center design was divided into smaller parts. The two main design tasks were to plan the external & internal design for the data center. External design covers following topics: physical space requirements, main and backup power, cooling, monitoring and access control, fire safety and external network cabling. Internal design covers: IT hardware requirements, racks & equipment space requirements, data center internal cabling, device cabling and future extensibility. These two designs are partially dependable on each other so they need to be cross-referenced before implementation. The design was concluded together with multiple infrastructure personnel along with the local facility support. The following chapters go through in more detail the summary of data center design implementation, which can be found in table 6. Organization reserved rights to the more detailed data center design and therefore only summary table of the configuration is shown.

TABLE 6. Summary of the data center design implementation

<b>Design</b>	<b>Implementation</b>
IT Hardware	Calculated to be able to provide operations for local applications and business critical applications with fault redundancy
Racks	Hardware is easily installable to the purchased racks from both sides and optional space calculated for a new rack
Datacenter internal cabling & device cabling	Internal cabling from rack to rack with ethernet and fiber cables. Device cabling using suitable length copper or fiber to the connection panels
Physical space requirements	Able to meet required space requirements for hardware devices with room for growth. Adequate airflow within the room estimated
Fire safety	Installed automatic fire safety system to put out any possible fire hazards. Fire safety system requires manual intervention when entering space to make it safe for personnel operating in the space
External network cabling	Duplicated network cabling via two different routes into the data center. Additional cable routes for possible error situations or future growth
Main and backup power	Datacenter located next to a transformer substation. Large UPS has been installed to provide power into the data center in case of power outage and additional building backup power is handled with diesel generators
Cooling	Duplicated and dedicated cooling devices providing standard temperature of 21 degrees Celcius
Monitoring and access control	Access to the data center is by personal ID-card. Emergency entry allowed with a single physical key. Data center is monitored with a security camera by an external security company

### 5.3.2 External datacenter design

Physical space requirements for data center include the actual location of the data center. For best possible outcome, the data center was located on a central position regarding network cabling to keep distance between on-site cabling to a minimum. Data center needed to be located on the bottom floor or with an access to a goods lift, which provides good accessibility for large and heavy hardware. There were two alternatives that were close enough to the necessary power sources, so the choice was done based on the location of network cabling. The actual data center room was measured to have enough room for standard rack installations, which allows operations on both sides of the racks. There is also some room for future growth. Single row of racks was installed, so there was no requirement to plan for additional space between rack rows.

In addition to physical space requirements, other external factors for the data center were also included in the design. Even small data centers require huge amounts of power, so the data center was placed next to a power source which cuts down costs for power cabling. To ensure uninterrupted power for the data center, an UPS was installed in the near vicinity. The buildings main power source is also backed up by diesel generators in case the UPS runs out of power.

Due to the location and hardware, data center was also estimated to generate a lot of heat, so adequate airflow was planned. Duplicate cooling devices that were separated from the buildings ventilation system were installed to provide continuous temperature of 20 degrees Celsius in the data center. Data center room was also equipped to deal with fire hazards by installing inert gas system to deprive oxygen in case of a fire.

As a safety feature, monitoring and access control to the physical space was implemented. Access control to the data center was limited to key cards and to a single physical key for safety precaution. Physical key access is a requirement set by the fire safety rules in Finland. Data center



was also equipped with security cameras to record any activity within the room. External provider was chosen to monitor the access into the physical space and the security footage is saved on a remote location.

External network cabling to the data center was duplicated for possible hardware failures. Data center was built with two external connections to ensure operability even when one outside route is having issues with its traffic flow. Additional empty fibre cabling was also installed for future usage.

### 5.3.3 Internal datacenter design

Designing most cost-effective solution for the internal hardware required a lot of background knowledge from the business. The hardware calculations enabled to plan the physical space calculation, power calculation and interconnectability. These factors also provided the answer how much rack space is required and will the physical space be able to meet the requirements.

The amount of racks also leads the planning for internal data center cabling. Having the power and network cabling available directly from the racks was a desired feature, so all the cables were routed above the rack as can be seen in the image 1.



IMAGE 1. Rack overhead cabling

By having internal rack to rack cabling installed, meant that future equipment could be installed more quickly and costs for these installations would be kept to a minimum. Image of the internal cabling can be seen in the image 2. The top four units are for internal cabling. Having both copper and fiber cabling between racks ensured that the equipment in racks can be changed without having to touch the data center internal cabling. New equipment can also be installed on any rack and these devices will still have the possibility to be connected to any of the pre-installed devices without installing any new interconnecting cabling.



IMAGE 2. Internal rack cabling with a router during initial installation

By implementing every part of the internal design in a way that it allows the data center to grow without having to change the internal layout in a radical way, means that future implementations can be done with minimal hardware costs and personal resources. Design was made with an aim to the future, which enables the organization to rapidly increase their data center capacity without any huge investments.

#### 5.4 Cluster with shared storage

The disaster recovery site is built using Lenovo and IBM products with VMWare virtualization. Two Lenovo x3650 M5 servers are installed as a cluster and redundant SAS cabling is used to connect IBM Storwize V3700 Storage to the cluster. Configuration from the front can be seen in image 3.



IMAGE 3. ESXi hosts and storage installed into a rack.

Since the racks have enough space above and below the devices, future installations for expansions or new hardware can be done without having to move the old equipment beforehand. Cabling from servers to the network devices is achieved by using a mixture of copper- and fiber-cabling. Logical level configuration was done to the disaster recovery site in a way that it would be possible to run virtual machines as if they were located on primary site. Specification for a single Lenovo server can be seen in the figure 13.


General		Resources													
Manufacturer:	LENOVO	CPU usage: <b>246 MHz</b>	Capacity 20 x 2,299 GHz												
Model:	System x3650 M5: 	Memory usage: <b>9845,00 MB</b>	Capacity 539837,90 MB												
CPU Cores:	20 CPUs x 2,299 GHz	Storage													
Processor Type:	Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz	<table border="1"> <thead> <tr> <th></th> <th>Status</th> <th>Drive Type</th> </tr> </thead> <tbody> <tr> <td>LUN_1</td> <td>✓ Normal</td> <td>Non-SSD</td> </tr> <tr> <td>LUN_2</td> <td>✓ Normal</td> <td>Non-SSD</td> </tr> <tr> <td>LUN_3</td> <td>✓ Normal</td> <td>Non-SSD</td> </tr> </tbody> </table>			Status	Drive Type	LUN_1	✓ Normal	Non-SSD	LUN_2	✓ Normal	Non-SSD	LUN_3	✓ Normal	Non-SSD
	Status	Drive Type													
LUN_1	✓ Normal	Non-SSD													
LUN_2	✓ Normal	Non-SSD													
LUN_3	✓ Normal	Non-SSD													
License:	VMware vSphere 5 Enterprise Plus - Licensed for 2 physic...	Network													
Processor Sockets:	2	<table border="1"> <thead> <tr> <th></th> <th>Type</th> </tr> </thead> <tbody> <tr> <td>NET-000-000</td> <td>Distributed port group</td> </tr> <tr> <td>NET-000-000</td> <td>Distributed port group</td> </tr> <tr> <td>NET-000-000</td> <td>Distributed port group</td> </tr> </tbody> </table>			Type	NET-000-000	Distributed port group	NET-000-000	Distributed port group	NET-000-000	Distributed port group				
	Type														
NET-000-000	Distributed port group														
NET-000-000	Distributed port group														
NET-000-000	Distributed port group														
Cores per Socket:	10														
Logical Processors:	40														
Hyperthreading:	Active														
Number of NICs:	6														
State:	Connected														
Virtual Machines and Templates:	1														
vMotion Enabled:	Yes														

FIGURE 13. Single x3650M5 server specifications from VMWare

### 5.4.1 Cluster storage configuration

To achieve the most usable space from a 48-disk configuration in a Storwize V3700 device, required the storage to be split into two pools. In the figure 14 you can see the total capacity from which was achieved using 4Tb disks. Three logical unit number (LUN) configurations were made so that the space increases per LUN would be more controllable. Capacity starts with 8Tb configuration and it can grow automatically until it hits pre-defined limit. This is to ensure that the total capacity is kept at minimum and to test that the auto grow settings work as intended. Each LUN has been mapped to the ESXi hosts by using Small Computer System Interface (SCSI) ID starting from number ten (one-zero) because SCSI ID zero is usually reserved for internal purposes of devices.

Name	State	Capacity
Pool0	Online	108.58 TiB
Pool1	Online	28.92 TiB

Name	State	Pool	UID	Host Mappings	Capacity
LUN1	Online	Pool0	6005076300808E33C000000000000001	Yes	8.00 TiB
LUN2	Online	Pool0	6005076300808E33C000000000000002	Yes	8.00 TiB
LUN3	Online (formatting)	Pool1	6005076300808E33C000000000000003	Yes	8.00 TiB

Host Name	SCSI ID	Volume Name	Volume Unique Identifier	Caching I/O Gr...
10.10.10.10	10	LUN1	6005076300808E33C000000000000001	0
10.10.10.10	12	LUN3	6005076300808E33C000000000000003	0
10.10.10.10	11	LUN2	6005076300808E33C000000000000002	0
10.10.10.10	12	LUN3	6005076300808E33C000000000000003	0
10.10.10.10	10	LUN1	6005076300808E33C000000000000001	0
10.10.10.10	11	LUN2	6005076300808E33C000000000000002	0

FIGURE 14. Storage pool configuration

#### 5.4.2 Cluster network configuration

Disaster recovery situations can be challenging if the network configuration needs to be changed during recovery. To achieve the easiest DR situation, the ip address range needs to be transferrable from the primary site, to the recovery site or the ip address range needs to automatically change during restore operations. This requires the underlying network to support the traffic routing regardless of the location of the virtual machine.

For achieving the same situation on a logical level, VMWare provides a logical device called VMware vSphere Distributed Switch (VDS). Downside for the virtual device is that only vSphere Enterprise Plus supports the vNetwork Distributed Switch. Also using the same VDS name is impossible on different data centers, so all hosts using the same VDS configuration need to be under the same data center regardless of their actual location which might lead to confusion if the VMWare data centers are named based on their physical locations. The benefit from using VDS is that the network configuration is always identical between the hosts that share the VDS. The standard logical switch does not support this, which may lead to virtual machine connection problems in a cluster fail-over situation, due to human error in configuration.



In the figure 15 you can see the logical cabling which is used to connect servers and storage to the physical network. In the physical environment, the cabling goes through interconnected cables between racks and connects to the actual devices in the data center or outside the data center.

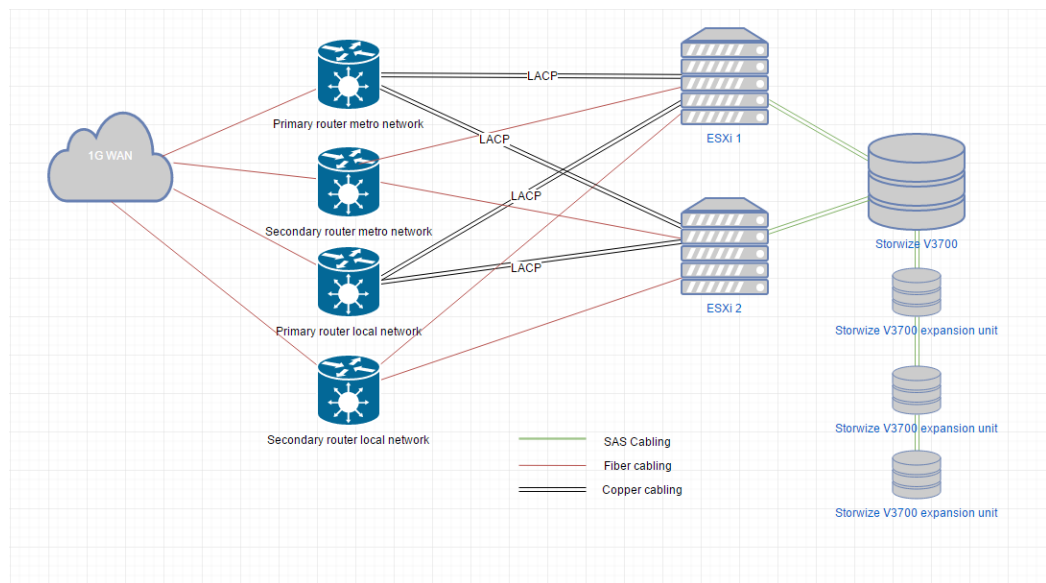


FIGURE 15. Logical cabling for cluster setup

VDS was configured based on the VMWare documentation and the logical cabling design. VDS uses multiple network adapters for different uplinks, and it also has multiple VLANs for different virtual machine traffic as can be seen in the figure 16. VMware standard switches can be used at the same time as VDS, but they need to be binded to different physical network adapters, which usually means that the organizations do not usually use both, because of the lack of physical devices on the underlying hardware.



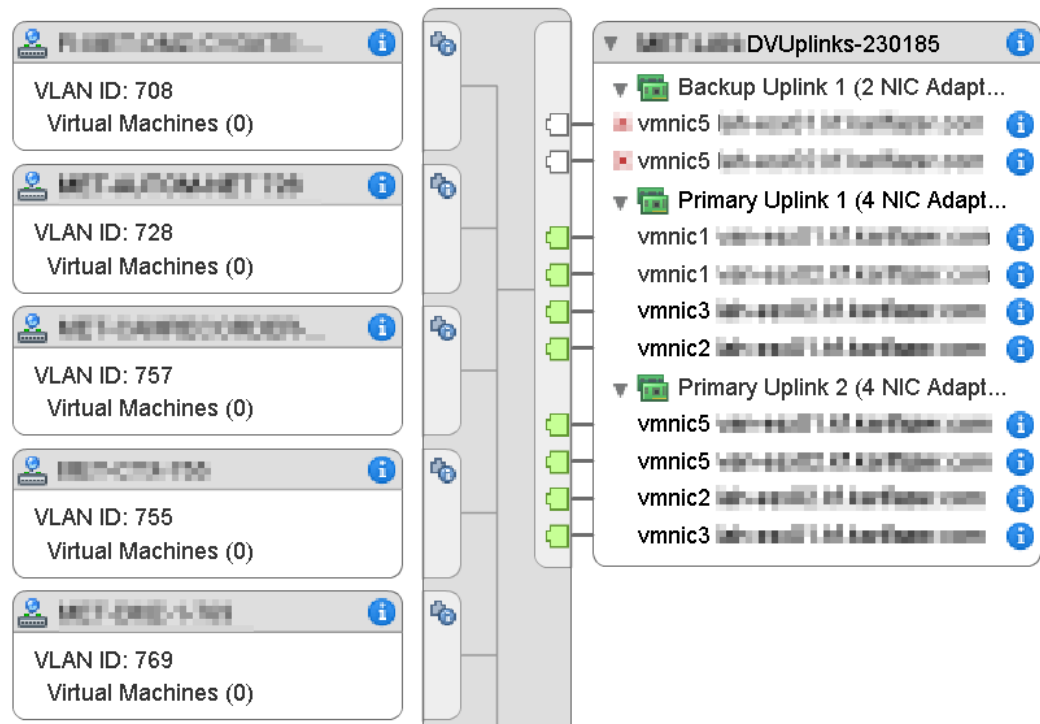


FIGURE 16. Partial image of the VDS topology

## 5.5 Disaster recovery

When planning for a data center disaster recovery, an engineer needs to start thinking the situation in a way that what if a site is lost, then what. The data center connectivity and hardware was designed with disaster recovery in mind, so it was crucial to find a software which could be used to accomplish the same in the logical layer. There are currently many good products to be used for backing up your virtual infrastructure and to prepare for disasters within your main data center.

Organization wanted a software that could handle increased workload, be easy to manage, have bandwidth control, have reasonable acquisition price, be able to work with NetApp and Storwize storages and that it would be compatible with both VMWare and Hyper-V virtualization. The program that met all the backup and disaster recovery requirements was Veeam. Veeam is built solely for virtual environments which run with VMware or Hyper-V. In 2016 Veeam was also included as one of the Leaders in the Gartner Magic Quadrant for Data Center Backup and Recovery Software.

Veeam can take normal virtual machine backups, but what makes it ideal for disaster recovery, is its capability to do so called SureBackups. A SureBackup job is a task for recovery verification, which makes it ideal for disaster recovery testing while doing backups. The process is done within Veeam's virtual lab environment, which means that normal operations aren't affected by any testing and it can be done one machine or with a group which makes close normal environment testing very easy.

All the backup jobs done with Veeam use VMWare tags. Tags are used to mark virtual machines with metadata, which Veeam backup jobs can read. Backups jobs are created to operate with these tags, which means that adding or removing virtual machines from backup routines only requires a removal of a tag in VMWare, rather than altering the whole backup job in Veeam. This makes manageability easier for the future. Multiple tags can exist on a single virtual machine, so doing for example daily, weekly and monthly backups only require adding of three tags to the virtual machine. An example of these tags can be seen on figure 17.

Tag Name	Category	Description
STP1-W2200-RP04	Backup	St. Petersburg Destination 1 every friday 22:00. Retention policy last 4
STP1-D2200-RP07	Backup	St. Petersburg Destination 1, every day 22.00. Retention Policy last 7
LT13-D0400-RP07-SQL	Backup	Lahti Destination 3, every day 04.00, Retention Policy last 7, SQL servers
LT11-DR2200-RP07	Backup	Lahti Destination 1, every day 22.00, Retention Policy last 7, Disaster re...
LT11-DR2000-RP02-TEST	Backup	TEST Lahti Destination 1, every day 20.00, Retention Policy last 2, Disa...
LT11-DR0300-RP07-AD	Backup	Lahti Destination 1, every day 03.00, Retention Policy last 7, Active Dire...

FIGURE 17. VMWare tag examples

VMWare tags and VeeAM jobs are using the same name and description. Every backup tag has been placed in category backup. The tag naming is based on three or four values

1) Backup repository suffix

IE: Repository VEEAM-STP1 -> Suffix STP1

2) Backup/DR type + start time

Default options

DR = Disaster recovery, sure backup

D = Daily

W = Weekly

M = Monthly

IE: D2200 or DR2300

3) Restore Points availability with two digits

IE: RP04

4) Specific system backup such as AD or Exchange

IE: AD

Complete naming examples:

STP1-D2200-RP04 (common)

STP1-D2200-RP04-AD (active directory)

STP1-DR2200-RP04 (disaster recovery)

The surebackup jobs are always linked to a certain backup job. This means that for example testing AD Backups requires a creation of a Veeam virtual lab and linking the AD Backup job into this surebackup job. The surebackup job runs independently and verifies whether the domain controllers seem to be healthy after being powered on based on the criteria defined, and sends a report to the technician about the whole process.

## 5.6 Disaster recovery RTO, RPO and testing

For the initial disaster recovery plan, the following jobs were defined:

LTI1-DR0300-RP07-AD, Active Directory surebackup

LTI1-DR2200-RP07, Disaster recovery surebackup

All the business applications rely on active directory authentication, so backing up AD is essential for bringing any services on-line in secondary data center. In the figure 18 there is an example how it is possible to view which jobs are linked to surebackup job and in which virtual lab do they run on. Virtual lab has been configured in a way that it provides the same network configuration as the virtual computers would normally have, but in a way that virtual machines have no external connectivity during testing. Accidentally bringing a copy of a domain controller on-line on normal network, could cause wide spread problems within the domain. However, without testing virtual machines on their normal network, it is impossible to know whether the backups are functional. This is where surebackup saves a lot of manual work from the data center specialist.

NAME ↓	PLATFORM	STATUS	LAST RESULT	NEXT RUN	APPLICATION GR...	VIRTUAL LAB	LINKED JOBS
AD SureBackup Lahti	VMware	Stopped	Success	21.11.2016 5:00:00		Virtual Lab - Lahti	LTI1-DR0300-RP07-AD
DR SureBackup Lahti	VMware	Stopped	Success	21.11.2016 0:00:00		Virtual Lab - Lahti	LTI1-DR2200-RP07

FIGURE 18. Surebackup jobs

VeeAM can pull backups from Netapp storage snapshots, which is used in the primary data center. This means that the backups will not cause any excess I/O for the virtual servers running business applications, since the data is being read from an already made storage snapshots. There underlying tasks on the storage device usually have no effect on the running virtual machine when using storage snapshots.

Real world backup jobs sometimes differ from expected results. Below you can see the difference between two jobs that have the same number of servers to process. First task LTI1-DR0300-RP07-AD figure 19 has six standardized domain controllers and the second task LTI1-DR2200-RP07 figure 20. has six application servers. Transferred data is the amount of data moved after compression and deduplication. In domain controller task, the amount of data is twice to the application server backup, but the transferred amount of data is six times bigger. If the application server job would run twice with same results, it would lead up to roughly 600Gb data which would take about 1h 18min. This is half an hour faster than the domain controller backup with roughly the same amount of data. Since the underlying storage and network is also roughly the same and they have the same kind of load, a conclusion can be drawn that the type of data to be backedup has the most effect on the actual backup time.

## Virtual machines: 6 domain controllers

- Duration: 1h 50min 35s
- Processing rate: 15 Mb/s
- Processed: 631,9 GB
- Read: 63,1 GB
- Transferred: 21,0 GB (3x)
- Throughput: 136,9 MB/s

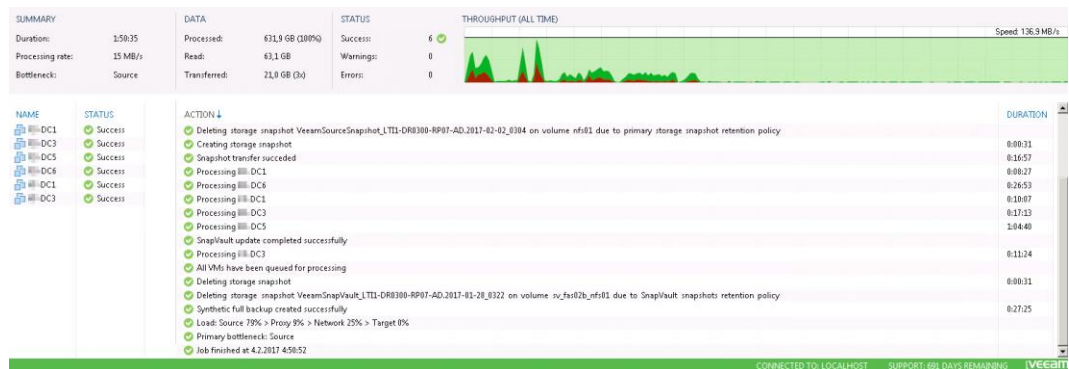


FIGURE 19. Active Directory surebackup summary

## Virtual machines: 6 application servers

- Duration: 39 min 17s
- Processing rate: 9 Mb/s
- Processed: 299,0 GB
- Read: 10,8 GB
- Transferred: 3,3 GB (3,3x)
- Throughput: 20,8 MB/s



FIGURE 20. Disaster recovery surebackup summary

Based on the results gathered, the values were inputted into Veeam's bandwidth calculator. The figures 21 and 22 below represent Veeam's suggestions for a WAN network that is necessary for the backup jobs to finish within a certain window. The change rate plays a major role even in here, cutting the network requirements to third for the application server backup job. Current backup RTO is set to 24 hours and there is no pressure for the backup jobs to finish, because there is a 1Gbit line between the sites.

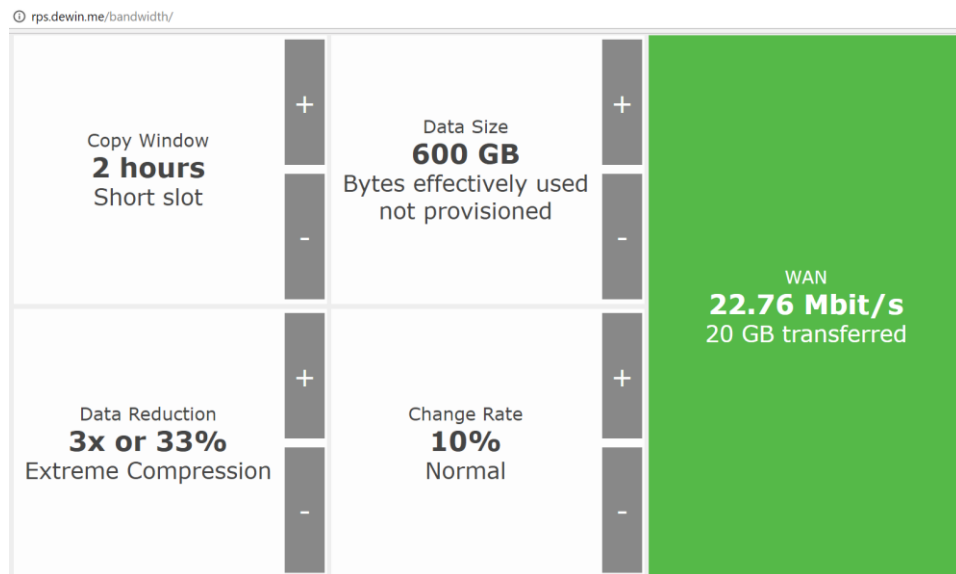


FIGURE 21. Bandwidth calculator domain controller job

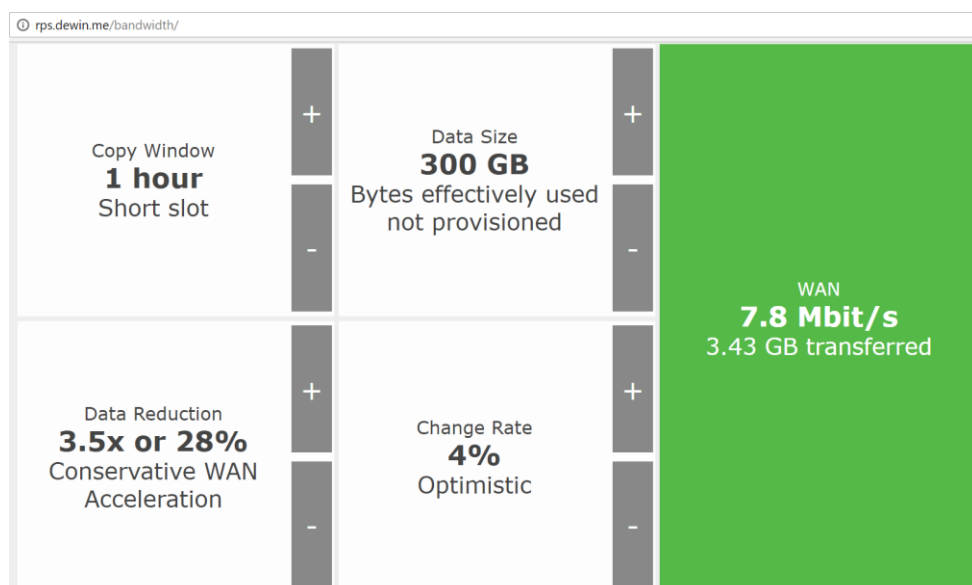


FIGURE 22. Bandwidth calculator application server job

For RPO the timing depends on many factors. With VeeAM it is possible to bring a faulty virtual machine on-line in less than 15 minutes. This works so that the VM is brought online directly from the backup created. Later, data center specialist can decide to recover this instantly recovered virtual machine into the normal datastore on the ESXi hosts. In the viewpoint of the virtual machines the RTO of under 15 minutes therefore is met, but since the virtual machines are on a secondary site, getting the business applications running requires that there is a network connectivity between the disaster recovery site and the main data center. Usually network design is done in a way that the crucial key points are installed in the data center. Therefore, the network connectivity to the primary site must be duplicated in a way that the primary data center can be fully offline, for example in a power outage situation, and the business applications are still able to run from the disaster recovery site.

Disaster recovery falls always under the major incident management process. The main goal is always to bring the services online on the primary site using backups that are located on-site. In a case where the services cannot be brought online in the primary data center, according to the organizations major incident process the decision for disaster recovery is made by the assembled major incident group. After the services are brought online on the disaster recovery data center, they are closely monitored and verified for normal operations. After the problems on the primary data center have been solved, all the services will be migrated back into their original location. The lifespan for disaster recovery situation is largely defined by the scale of the problem or problems and it can be anything from minutes to days, in worst cases even in weeks.

Testing, training and preparing for these events from a data center perspective should be done periodically to avoid any excess downtime with the business applications. Ensuring data center specialist are aware of the technical tasks they need to perform during disaster recovery and



that they have the necessary knowledge, falls into their supervisors' responsibility.

## 5.7 Documentation

For every ICT project to be successful and in a state where it can be transferred from a project state into a running service, proper documentation is required. The baseline for this disaster recovery projects documentation was to create a common service model for all business units for business continuity. This documentation was to support the previously defined major and critical incident workflow within the organization.

The four major objectives defined were: resolution, communication, sufficient resources and post incident review. To achieve these requirements every system supported by normal major incident management process was required to define business contact person, possible service provider contact information and the process for error handling. This documentation was to cover every normal anomaly within the system and how to recover from it, as well as define a technical process when the given guidelines do not provide an answer to that problem.

To ensure the documentation is kept up to date, every supported system by disaster recovery is required to have a yearly checkup on the status of the system and its documentation. In addition to this yearly checkup, business owners are required to handle governance model together with ICT management as well as do controlled change management together with ICT and possible application vendors. With structured and well documented service management, the organization aims to swiftly recover from any possible disaster recovery situation and return to normal operations as quickly as possible.

## 6 CONCLUSIONS

### 6.1 Case study result analysis

The case study relied heavily on design science approach as well as previously gathered knowledge working with data centers and data center hardware. RPO and RTO times were controlled by the defined budget and the budget was defined based on a rough estimate on what the requirements for the DR site were and what could be accomplished within a certain amount of budget. These estimates cannot be presented in this thesis, since they contain organization limited information. What can be said about the estimates is that multiple options were presented for the business and the decision for the acceptable level for the DR solution were made by the top management. These decisions were then followed in the technical implementation.

The initial estimates for the possible RPO and RTO times were achieved and requirements set by the business were met. The case study was limited to only building the DR solution for business-critical solutions, but the technical solutions allows expanding this scope to other solutions even with the currently installed hardware. This scope expansion is considered easy from the technical point of view and the main challenges which scope expansion are to document and implement the business solutions in a way that they are compliant with the organizations DR and MIM processes.

Both ICT personnel and the business agreed that the implemented solution for disaster recovery and how it supports the pre-defined major incident management allows the business continuity to reach new levels within the organization. DR is currently a standard service that is offered within the organization based on the business needs. Due to the implemented guidelines, different services can be added into the DR scope in a controlled manner.

For future development, there is the aim to expand the DR solution to other sites as well as do yearly testing for every service covered by the DR scope. Initial study has already been started for site expansion.

## 6.2 Research questions and discussion

The current IT world is becoming more virtualized, more 24/7, more user oriented. There has been a birth for a whole new requirement set for companies and organizations to ensure their environments are always working. Having systems always up and running is a necessity for many organizations, which in turn has brought forth clear demand for working disaster recovery solutions. People expect things to just be working all the time and for example web-sites with information of a system downtime, are becoming a thing from the past.

How to ensure business critical service continuity within data center platform?

Disaster recovery and major incident management have become cornerstones for many companies' livelihood. Without working systems, the companies may lose a lot of revenue, even be faced with a situation where they need to close their operations completely. Even companies that do not suffer financially might suffer a huge blow to their image when the information customers are seeking is not ready right away.

Building a disaster recovery site is like buying a very good insurance. However, just like with any other insurance it is not cheap and the benefits only show themselves after an incident has happened. In addition, just like insurances need a check-up every now and then, so does the disaster recovery and MIM process. Building the actual disaster recovery site is a very challenging task to be done because in the end that system is the one that needs to be working when everything else fails. Current data centers are usually built with redundancy in mind, but there are cases when the redundancy does nothing if the whole site itself is lost. There is

also always the possibility for data corruption or an outside threat which may require for companies to result into using their disaster recovery solutions.

Which technical solution for data center platform should be utilized and where?

The goal for disaster recovery should always be to start by building the primary data center with redundancy in mind and to keep backups technically close, so normal incidents can be solved quickly. Disaster recovery processes from a secondary data center, whether that data center is in-house or an external one such as Microsoft Azure or Amazon Web Services, usually always take too long for business-critical applications due to the network connectivity and possible technical challenges. These problems can be mitigated to a certain degree, but geographical challenges are always an obstacle which data center specialist need to be aware of. In today's data centers, a single point of failure is no longer acceptable and every component should be built with redundancy or with a possible fail-over mechanism.

Choosing the technical solution for a data center platform is mostly defined by the business needs and the budget at hand. These things together define the acceptable level for a possible service or data loss. ICT specialist are usually required to present alternative solutions in which they specify how much would a certain level of data security cost. With top of the line solutions you can build systems that are able to handle software or hardware failures with zero to very low data loss and in most cases, with zero business impact. While the cheapest options, while providing some form of recovery, always mean that there is certain amount of data loss and the recovery process itself takes time. Whatever the level of business impact agreed may be, an ICT specialist should always look for the technical solutions which aim to be futureproof and as compatible as possible. By doing this it is possible to some extent ensure that whichever way the technical solutions develop, there is always the

possibility of upgrading your DR solutions with minimal costs.

How long will it take to implement identified solutions?

Implementation of a chosen technical solution can take anywhere from few weeks up to several months. If an organization already has the technical requirement met for example to a cloud service provider, setting up a disaster recovery from a technical point of view is a very quick process. The same cannot be said for building an actual disaster recovery data center, since in most cases the actual physical space needs to be prepared or possibly built before any technical solution can be made. The challenge with any DR solution is the testing process, which usually requires some form of business participation to ensure that the DR plan is working as intended. This testing process should be counted into the implementation process, since it is the only possible way of ensuring the data is secure and accessible. The timeline for the implementation can therefore be vastly extended and take up a lot of resources.

How to make a common service model for all business units for business continuity?

When an organization decides to invest in a DR solution, there is usually one or few main systems which the DR aims to cover in the initial launch. ICT professionals therefore need to be already beware of the possible expansion for new requirements and design the solution in a more universal matter. Aiming for tools and solutions which can cover all, but the most complex and closed systems which require special solutions, should be the key aim. When the correct technical solutions are in place, it is easy to create or follow a common service model for all business needs. ICT personnel usually need to engage the business to understand that business continuity is more than a technical solution, it is a way to do business that is sustainable in every possible situation.

How to ensure documentation is always up to date regarding business continuity?

A properly designed and implemented service model serves the business as well as the ICT personnel in finding the solutions to keep the wheels rolling. DR however is not a thing that can just be done, it is a continuous joint effort from the whole organization. Whether it is the documentation, the actual processes or the training required for the personnel, these tasks are never done. Continuous review and update to the implemented services and solutions is the only way to ensure business continuity. Depending on the organization it can be a weekly, monthly or a yearly task, but it is a requirement that must be met or all the previous hard work in implementing a DR solution can be lost.

Major incident management or disaster recovery, neither of these crucial elements are not achieved by simply snapping ones' fingers. These things require a change in the way of thinking, a change in how to ensure there will be tomorrow for the organization. Ensuring that the way of working can continue even tomorrow is a choice and it is achievable, while sometimes it might take time and resources to do so. By not achieving a situation where there is a continuity process and an environment for it to take its place, can be devastatingly costly. There is a common goal to keep the wheels rolling and it can only be achieved by working together.

## REFERENCES

### Written references:

Hevner, A. & Chatterjee, S. 2010. Design Research in Information Systems: Theory and Practice. US: Springer.

Kuechler, B., & Vaishnavi, V. 2008. On theory development in design science research: anatomy of a research project. UK: Palgrave Macmillan.

### Electronic references:

20000 Academy. 2016. What is ISO 20000. [referenced 15.10.2016]. Available at [https://advisera.com/wp-content/uploads/sites/6/2016/02/What\\_is\\_ISO\\_20000\\_white\\_paper\\_EN.pdf](https://advisera.com/wp-content/uploads/sites/6/2016/02/What_is_ISO_20000_white_paper_EN.pdf)

ASHRAE Technical Committee. 2011. Thermal Guidelines for Data Processing Environments – Expanded Data Center [referenced 26.8.2017] Available at [ecoinfo.cnrs.fr/IMG/pdf/ashrae\\_2011\\_thermal\\_guidelines\\_data\\_center.pdf](http://ecoinfo.cnrs.fr/IMG/pdf/ashrae_2011_thermal_guidelines_data_center.pdf)

Amiel, T., & Reeves, T. C. 2008. Design-Based Research and Educational Technology: Rethinking Technology and the Research Agenda. [referenced: 15.10.2016] Available at [http://www.ifets.info/journals/11\\_4/3.pdf](http://www.ifets.info/journals/11_4/3.pdf)

Bahan, C 2003. The Disaster Recovery Plan [referenced 15.10.2016]. Available at <https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-1164>

Belden Inc. 2009. Data Center Cabling Guide. [referenced 14.8.2017] Available at <http://www.belden.com/pdfs/Catalogs/DataCenterCablingGuide.pdf>

Bell, M. 2005 Use Best Practices to Design Data Center Facilities [referenced 20.10.2016]. Available at <https://www.gartner.com/doc/476880/use-best-practices-design-data>

Bertolucci, J. 2013. Big Data Analytics: Descriptive Vs. Predictive Vs. Prescriptive. [referenced: 15.10.2016] Available at <http://www.informationweek.com/big-data/big-data-analytics/big-data-analytics-descriptive-vs-predictive-vs-prescriptive/d/d-id/1113279>

BraunsBlog. 2012. Major Incident Handling [referenced 15.10.2016]. Available at <http://braunsblog.com/sitebuildercontent/sitebuilderfiles/majorincidenthandlingplan.pdf>

Brocade Communications Systems. 2007. Best Practises Guide: Cabling the Data Center. [referenced 14.7.2017] Available at <https://www.brocade.com/content/dam/common/documents/content-types/product-design-guide/cabling-best-practices-ga-bp-036-02.pdf>

Cisco. 2017. Cisco Unified Computing System Site Planning Guide: Data Center Power and Cooling [referenced 3.5.2017] Available at [https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/unified-computing/white\\_paper\\_c11-680202.pdf](https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/unified-computing/white_paper_c11-680202.pdf)

Cisco Systems, Inc. 2006. Data Center Disaster Recovery [referenced 15.10.2016]. Available at [http://www.cisco.com/c/dam/global/en\\_my/training-events/cnsf/files/T2-S2\\_KwaiSeng-DRv2.pdf](http://www.cisco.com/c/dam/global/en_my/training-events/cnsf/files/T2-S2_KwaiSeng-DRv2.pdf)

Clark, J. 2014. Data center design primer: Part three [referenced 20.10.2016]. Available at <http://www.datacenterjournal.com/data-center-design-primer-part-3/>

Commscope. 2014. Innovative Data Center Lighting Solutions. [referenced 13.10.2016]. Available at [http://www.globalsecuritymag.fr/IMG/pdf/WP-107631-EN\\_InnovativeData.pdf](http://www.globalsecuritymag.fr/IMG/pdf/WP-107631-EN_InnovativeData.pdf)



Commscope. 2015. Data center cabling design fundamentals. [referenced 15.10.2016]. Available at [http://www.commscope.com/DP/WP-321067-EU-Data\\_Center\\_Cabling\\_Design\\_Fundamentals.pdf](http://www.commscope.com/DP/WP-321067-EU-Data_Center_Cabling_Design_Fundamentals.pdf)

CtrlTech. 2016. Data Center Fire Suppression. [referenced 15.5.2017]. Available at <http://www.datacenter-serverroom.com/fm200-fire-suppression-data-center-design>

Diminico, C. 2006. Telecommunications Infrastructure Telecommunications Infrastructure Standard for Data Centers [referenced 15.10.2016]. Available at [http://www.ieee802.org/3/hssg/public/nov06/diminico\\_01\\_1106.pdf](http://www.ieee802.org/3/hssg/public/nov06/diminico_01_1106.pdf)

Dugmore, J. & Holt, A. 2016. ISO/IEC 20000 and ITIL – The Difference Explained [referenced 15.10.2016]. Available at <https://www.tsoshop.co.uk/parliament/bookstore.asp?FO=1229332&DI=571307>

Dumitru, M. 2017. Best Practice Network Design for the Data Center. [referenced 14.7.2017] Available at [https://www.cisco.com/c/dam/global/ro\\_ro/assets/ciscoexpo/2010/src/docs/presentations/12.pdf](https://www.cisco.com/c/dam/global/ro_ro/assets/ciscoexpo/2010/src/docs/presentations/12.pdf)

ECD Solutions. 2017. Data centre monitoring and management [referenced 20.10.2016]. Available at [www.ferret.com.au/ODIN/PDF/Showcases/107839.pdf](http://www.ferret.com.au/ODIN/PDF/Showcases/107839.pdf)

England, R. 2014. what is an ITSM Major Incident? ITIL doesnt say. [referenced 15.10.2016]. Available at <http://www.itskeptic.org/content/what-itsm-major-incident-til-doesnt-say>

Enisa. 2010. Good Practice Guide for Incident Management [referenced 15.10.2016]. Available at [https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management/at\\_download/fullReport](https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management/at_download/fullReport)

European Commission. 2017. ICT standardization. [referenced 26.8.2017]  
Available at [https://ec.europa.eu/growth/industry/policy/ict-standardisation\\_fi](https://ec.europa.eu/growth/industry/policy/ict-standardisation_fi)

Hu,P. 2017. Electrical Distribution Equipment in Data Center Environments. Available at [http://www.apc.com/salestools/VAVR-8W4MEX/VAVR-8W4MEX\\_R1\\_EN.pdf](http://www.apc.com/salestools/VAVR-8W4MEX/VAVR-8W4MEX_R1_EN.pdf)

IEEE. 2017. Climate change concerns and Finnish electric power supply security performance. [referenced 02.08.2017]. Available at <http://ieeexplore.ieee.org/document/7856318/>

Invest in Finland. 2016. Build your next data center in Finland. [referenced 15.10.2016]. Available at <http://www.investinfinland.fi/datacenter/main.php>

ITIL Service Management. 2011. ITIL Major Incident - All you want to know [referenced 15.10.2016]. Available at <http://itservicemngmt.blogspot.fi/2011/03/itil-major-incident-all-you-have-to.html>

Jew,J. 2016. Data Center Practices [referenced 21.10.2016]. Available at [https://www.bicsi.org/uploadedFiles/BICSI\\_Website/Global\\_Community/Presentations/CALA/Jew\\_DC\\_mexico\\_2016.pdf](https://www.bicsi.org/uploadedFiles/BICSI_Website/Global_Community/Presentations/CALA/Jew_DC_mexico_2016.pdf)

Lam, J. 2016. Metz Connect Breaking the rules. [referenced 15.10.2016]. Available at [https://www.bicsi.org/uploadedFiles/BICSI\\_Website/Global\\_Community/Presentations/Southeast\\_Asia/2.5%20Breaking%20the%20Rules.pdf](https://www.bicsi.org/uploadedFiles/BICSI_Website/Global_Community/Presentations/Southeast_Asia/2.5%20Breaking%20the%20Rules.pdf)

Lo Bosco,M. 2011. Effective Fire Suppression in Data Centers Requires Careful Planning by FMs. [referenced 15.10.2016]. Available at <http://www.facilitiesnet.com/firesafety/article/Effective-Fire-Suppression-in-Data-Centers-Requires-Careful-Planning-by-FMs-Facilities-Management-Fire-Safety-Feature--12580>

Martin, B. 2002. Disaster Recovery Plan Strategies and Processes [referenced 15.10.2016]. Available at <https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-strategies-processes-564>

Nolting, D. 2013. RPO, RTO, PTO and DRaaS: Disaster recovery explained. [referenced 15.10.2016]. Available: <https://www.bluelock.com/blog/rpo-rto-pt0-and-raas-disaster-recovery-explained>

NTT Facilities. 2017. Example of a data center layout. [referenced 15.10.2016]. Available at [http://www.ntt-f.co.jp/english/service/data\\_cor/](http://www.ntt-f.co.jp/english/service/data_cor/)

Panduit. 2014. Identification Solutions for Data Center Infrastructure [referenced 21.1.2017]. Available at <http://www.panduit.com/ccurl/996/880/data-center-id-infrastructure,0.pdf>

Patel,S. 2015. ISO 27001 Information Security Management System Checklist. [referenced 15.10.2016]. Available at <https://www.linkedin.com/pulse/iso-27001-information-security-management-system-checklist-patel>

PennWell Corporation. 2014. 3 reasons to use LED lighting in a data center. [referenced 15.10.2016]. Available at <http://www.cablinginstall.com/articles/2014/04/leds-in-datacenters.html>

Rasmussen, N. & Torell, W. 2015. Data Center Projects: Establishing a Floor Plan [referenced 12.7.2017] Available at [http://www.apc.com/salestools/VAVR-6KYMZ7/VAVR-6KYMZ7\\_R2\\_EN.pdf](http://www.apc.com/salestools/VAVR-6KYMZ7/VAVR-6KYMZ7_R2_EN.pdf)

Researchandmarkets. 2016. Data Center Construction Market in Western Europe 2015-2019 [referenced 15.10.2016]. Available at <http://www.researchandmarkets.com/reports/3383697/data-center-construction-market-in-western-europe#pos-0>

Robin, M. 2015. Fire Protection Options for Data Centres. International Fire Buyer. [referenced 15.10.2016]. Available at [https://www.chemours.com/FE/en\\_US/assets/downloads/pdf/201501-FireBuyerArticle.pdf](https://www.chemours.com/FE/en_US/assets/downloads/pdf/201501-FireBuyerArticle.pdf)

Rouse, M. 2015. disaster recovery site (DR site). [referenced 15.10.2016]. Available at <http://searchdisasterrecovery.techtarget.com/definition/disaster-recovery-site-DR-site>

Ryan, M., Brett Rucker, B., Nelson, D., Vlasaty, P., R, K.V., DeVito, S., & Day, B. 2009. Energy Efficient Datacenters electrical design. [referenced 14.7.2017] Available at <http://www.vinsure.in/pdf/data-center-optimisation-solution/electrical-design-data-center.pdf>

Scalet, S. 2015. How to build physical security into a data center. [referenced 15.10.2016]. Available at <http://www.csoononline.com/article/2112402/physical-security/physical-security-19-ways-to-build-physical-security-into-a-data-center.html>

Schulz, G. 2009. Data Center Measurement, Metrics & Capacity Planning [referenced 21.10.2016]. Available at <http://www.networkcomputing.com/data-centers/data-center-measurement-metrics-capacity-planning/1409405220>

Siemon. 2009. Data Center Cabling Considerations: Point-to-Point vs Structured Cabling. [referenced 3.5.2017] Available at [http://files.siemon.com/share-white\\_papers-pdf/09-06-18-data-center-point-to-point-vs-structured-cabling.pdf](http://files.siemon.com/share-white_papers-pdf/09-06-18-data-center-point-to-point-vs-structured-cabling.pdf)

Telecommunications Industry Association. 2012. Telecommunications Infrastructure Standard for Data Centers. [referenced 15.10.2016]. Available at <http://www.tiaonline.org/standards/buy-tia-standards>

The Design-Based Research Collective. 2002. Design-Based Research: An Emerging Paradigm for Educational Inquiry. [referenced: 15.10.2016] Available at <http://www.designbasedresearch.org/reppubs/DBRC2003.pdf>

Ucisa 2016. ITIL – Dealing with major incidents [referenced 15.10.2016]. Available at <http://www.ucisa.ac.uk/>

Vaidyanathan,K., Balaji,P., Wu,J., Jin,H., Panda,D. 2004. An Architectural study of Cluster-Based Multi-Tier Data-Centers. [referenced 21.10.2016]. Available at <http://mvapich.cse.ohio-state.edu/static/media/publications/abstract/vaidyana-arch-tr.pdf>

Valentic, B. 2016. ITIL and ISO 20000: A Comparison. [referenced 15.10.2016]. Available at <http://advisera.com/20000academy/knowledgebase/itil-iso-20000-comparison/>

Wold, G. 2013. Disaster Recovery Planning Process [referenced 15.10.2016]. Available at <http://www.disasterrecoveryplantemplate.org/disaster-resilience/disaster-recovery-planning-process/>