universität wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

„Business Continuity Management in Times of Crisis“

verfasst von / submitted by

Teresa Loreth, BSc

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Science (MSc)

Wien, 2021 / Vienna 2021

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	UA 066 914
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Masterstudium Internationale Betriebswirtschaft UG2002
Betreut von / Supervisor:	Univ.-Prof. Mag. Dr. Immanuel Bomze

This thesis is dedicated to my brother Maximilian

who is my most important sparing-partner,

even outside the tennis court.

Acknowledgements

Throughout my Master-Thesis-Project, I have received a great deal of support. – Now it´s time to say thank you.

First of all, I would like to thank my supervisor Univ.-Prof. Mag. Dr. Immanuel Bomze and my co-supervisor Univ.-Prof. Mag. Dr. Stefan Pickl whose insightful feedback really pushed me to sharpen my line of thoughts and finally brought my thesis to a higher level.

A very special word of thanks goes to the experts of the critical infrastructure organisations Deutsche Bahn, Deutsches Patent- und Markenamt and Österreichisches Rotes Kreuz.

Thank you so much for the insightful interviews, your provided information and especially for your time discussing with me. In this context, I would like to thank in particular:

- Deutsche Bahn

Burkhard Arnold, Angelika Oswald & Patrick Theurer
Corporate Security (IZ) and Business Continuity Management

- Deutsches Patent- und Markenamt (German Patent and Trade Mark Office)

Annette Kirchner
Head of Strategic Process Management (Stabstelle 0.3)

- Österreichisches Rotes Kreuz (Austrian Red Cross)

Michael Sartori
Landesrettungskommandant
Member of the Board Vienna Red Cross (Wiener Landesverband)

Table of Contents

CHAPTER I.

Introduction

It should be noted in the beginning that the present thesis does not constitute a representative empirical study. It is a large-scale case study of carefully selected organisations from the critical infrastructure sector in Austria and Germany.

1.1. Motivation of this Research

Based on the outbreak of the Covid-19 pandemic, many industries have been confronted with new challenges. In this context, the term business continuity became of great significance. From an organisation´s point of view the method of Business Continuity Management (BCM) became extremely relevant, as entrepreneurs, institutions, governmental authorities, etc. had to continue their businesses under extraordinary conditions. While certain sectors products have been suddenly high demanded; other industries were obliged to downtime their production overnight. In this context, particularly critical infrastructure organisations have been of significant importance, as they have been far more demanded than usually.

The Covid-19 pandemic illustrates how significant critical infrastructure organisations are in times of crisis and of what relevance their BCM-systems are. For this reason, the thesis focuses on critical infrastructure organisations that have been particularly under pressure in times of the pandemic and particularly analyses their BCM-systems. In this sense, challenges concerning Covid-19 were especially shown.

A qualitative analysis in form of expert interviews has been conducted with three critical infrastructure organisations. BCM-systems of Deutsche Bahn, Austrian Red Cross and German Patent and Trade Mark Office were analysed and data of the interviews has been gathered for further analysis. In this connection, a comparative analysis is conducted in a later part of the present thesis.

One of the interview outcomes was that the BCM-systems that are currently in-use reach their limits due to the issue of big data. High amounts and high-speed data slow down the systems. As a consequence, the system´s effectiveness decreases. Especially in times of crisis, when external economic conditions change, new challenges emerge. It was quickly clear, that for the improvements of BCM-systems a further tool is required.

Therefore, research has been conducted regarding a tool that supports and expands the BCM-systems. Hence, the Knowledge Graph has been identified and added to the thesis as it was considered a suitable tool that could support and expand the BCM-systems of the critical infrastructure organisations. The ambition was to develop a holistic KG that could be implemented to each BCM-system of Deutsche Bahn, Austrian Red Cross and German Patent and Trade Mark Office.

Within the scope of the present thesis, holistic KG-construction-methods were researched that could be applied to the BCM-systems of critical infrastructure organisations. Literature showed that there were various KG-construction-tools, like for instance Knowledge Graph Induction (KGI) by IBM[1]. However, it has been found that that the construction tools were mainly applied to single organisations. Furthermore, no literature has been identified that shows a KG application to more than one BCM-system of critical infrastructure organisation. Hence, a research gap has been determined.

[1] https://research.ibm.com/blog/knowledge-graph-ai

After the gap in literature has been identified the research question(s) could be formulated as follows.

Research Question(s)

- How does a template of a holistic Knowledge Graph for critical infrastructure organisation´s BCM-systems look like?
- What outcomes can be determined, when a holistic Knowledge Graph is applied to BCM-systems of critical infrastructure organisations?

The corresponding hypothesis to the research questions has been formulated as follows.

Hypothesis

- The implementation of a holistic Knowledge Graph to the BCM-systems of critical infrastructure organisations improves and expands the systems that are currently in-use at DB, Austrian Red Cross and DPMA.

The aim of the KG-construction which represents a first template that could be further developed by the individual critical infrastructure organisations, is to identify the most critical entities and their corresponding relations to each other. The empirical analysis connects the BCM part with the KG part by creating a holistic KG for the three critical infrastructure organisations interviewed. The construction of a holistic KG is intended to find out whether the hypothesis holds and to find answers to the research questions.

In the end, it becomes visible how the BCM-processes could be expanded by the application of the developed KG. This is illustrated with two examples that point out the functionalities of the developed Inner-Critical-KG –a holistic KG that could be applied to each BCM-system of Deutsche Bahn, Austrian Red Cross and German Patent and Trade Mark Office.

As part of the validation process concerning the establishment of the Inner-Critical-KG, a special workshop should have been held with the experts of Deutsche Bahn, German Patent and Trade Mark Office and Austrian Red Cross. Unfortunately, this was not possible due to the Covid-19 pandemic. Therefore, the validation process for the developed graph was conducted by a second interview round.

1.2. Structure of the Thesis

The following table provides an overview of the structure of the present thesis.

Introduction Crisis	**Expert-Interviews** (Deutsche Bahn, German Patent and Trade Mark Office, Austrian Red Cross)	**Theory BCM**	**Theory KG**	**Construction KG**

The main purpose for implementing BCM in an organisation is to improve a business´s capabilities to deal with a crisis. A crisis is considered the most severe type of an incident that a business is confronted with (Swissbanking 2013). Critical infrastructure organisations play a crucial role during times of crisis. Therefore, the focus of this chapter lies on the definition of crises, the severity of incidents, the crisis management and it especially concentrates on the difference between a crisis and the special scenario of a pandemic. In the end the challenges due to Covid-19 for Deutsche Bahn, German Patent and Trade Mark Office and Austrian Red Cross are presented.

The ambition of this chapter is to clearly illustrate the importance of BCM during times of crisis. For this reason, a certain figure will be added to the thesis that highlights the different procedures of an incident and the impacts of BCM. Figure 2 clearly points out that the importance of BCM during an incident is uncontroversial.

For linking the issues of crisis and BCM, a brief introduction about critical infrastructure organisations follows. In this context, the regulations for critical infrastructures in Austria as well as in Germany are shown.

The following chapter demonstrates the empirical component of the thesis. In this connection, a qualitative analysis has been conducted in the form of expert interviews with respect to the BCM-systems of Deutsche Bahn, German Patent and Trade Mark Office and Austrian Red Cross. In this part the BCM-systems of each organisation will be presented regarding the following aspects: BCM developments, BCM concerning the respective organisation, the responsibilities of BCM, BCM process, BCM in the context of risk (management) as well as potential threats and objectives. The section concludes with the expert´s needs and expectations after a tool that improves the current BCM-systems.

For summarizing the outcomes of the expert interviews, a table has been developed that captures the main characteristics of the BCM-systems of Deutsche Bahn, German Patent and Trade Mark Office and Austrian Red Cross. Characteristics regarding the developments, structure, responsibilities, threats, objectives, generated products, tasks, risk evaluation, decision-making-process and needs in the context of BCM were illustrated.

To provide a solid level of comprehension, the thesis will go into more detail about BCM. Chapter 4 provides information concerning BCM definitions, historical developments, different kind of risks, entrepreneurial resilience, BCM role in an organisation´s risk management, the operational risk management as well as the operational risk model, the idea of the BCM-lifecycle and their corresponding four components (understanding the organisation, determining a BCM-strategy, developing and implementing BCM response and exercising, maintaining and reviewing) will be presented. Afterwards, the chapter focuses on traditional BCM-tools like for example the business impact analysis (BIA) and its purposes. Then business continuity testing and business continuity planning follow. In the following

section the theoretical approach becomes more practical by the development of a business continuity management strategy, the definition of a business continuity management system and finally by the BCM embedding process to an organisation. In a next step the thesis strives to identify reasons for the malfunctioning of business continuity management systems. In this sense, critical success factors during the implementation phase, influencing variables and the multilateral continuity planning approach that represents one possibility to manage newly emerging influencing variables effectively are shown. In conclusion the objectives of BCM, the value of a BCM-plan and the critical success factors for long-term success are illustrated.

After providing a solid theoretical basis of BCM, the needs and expectations of the experts will be once again addressed in a brief summary to recall the basic situation of the BCM-systems regarding the data overload that decreases system´s effectiveness. The expectations by the experts set out that a further tool that improves the present BCM-system is required.

Based on this fact a Knowledge Graph will be implemented to the thesis. A KG illustrates real-world entities and their corresponding relations to each other (Paulheim 2016). The KG-Chapter gives insights of the idea of knowledge sharing, the connection between knowledge and AI, the concept of knowledge bases –and in this context the benefit of knowledge libraries. Besides it shows examples of KG as well as the three components of the KG-concept.

In order to provide the reader a better understanding of the representation of knowledge within a KG, it is relevant to take a closer look at three further theoretical concepts because the KG is related to various other theories. The Entity Relationship Model (ERM) by Edgar Codd, the theory of Semantic Networks and the idea of Ontologies are the main groundwork for the emergence of KGS and will be particularly analysed. Afterwards the thesis illustrates the idea of conceptual knowledge processing according to Wille (2006). Conceptual Knowledge Processing (CKP) is considered a method that seeks to the creation or identification of methods that could be applied for the processing of knowledge. It is considered a relevant component for the subsequently following first construction processes of a KG. The application process of KGs, the process of knowledge creation and the implementation of a knowledge graph management system and their corresponding prerequisites regarding the implementation process follows. This step is further divided into the selection of logical formalism, gathering and managing big data, and finally the procedural third-party code. In the end of the chapter DATALOG, a declarative programming language and VADALOG, a project-cooperation between Oxford University, University of Manchester, Edinburgh and industrial partners follow.

Finally, the Knowledge Graph Construction is the next step. A summary of the main characteristics that a KG has to fulfill that could be implemented to the BCM-systems of the critical infrastructure organisations interviewed, is briefly illustrated. The aim of this chapter is to develop a holistic KG that could be applied to the BCM-systems of DB, Austrian Red Cross and DPMA.

The KG construction process consists of the following three steps.

1. Gathering data of the expert-interviews for the creation of an organisation-specific KG. The construction process of the individual graphs has been carried out according to the knowledge-base-triple-method based on the approach by Rusu et al. (2007).
2. Comparing the individual KG to each other with a special focus on the identification of interfaces concerning entity-similarities. In this context, the input-important-scores-method by Park et al. (2019) has been applied for the identification of critical entities between the single KG of DB, Austrian Red Cross and DPMA.
3. Construction of the Inner-Critical-KG, a holistic KG that covers all of the identified critical entities. Subsequently the graph´s features will be analysed. A special focus will be placed on the critical entities within the Inner-Critical-KG and their classifications.

After the completion of the holistic KG, the functionalities will be tested with two different external influencing variables. For this reason, the thesis runs through the scenario of a pandemic and a blackout which hit the BCM-systems of the organisations interviewed.

Finally, the thesis concludes with some pointers to possible future prospects and further applications of the Inner-Critical KG will be discussed.

CHAPTER II.

Crisis

2.1. Definition

A crisis is an unexpected situation characterized by unstable conditions and an outlook that is unclear. Crisis could affect various areas, like for example political, social or economic belongings and stand for a sudden change of circumstances. Furthermore, it is seen as a situation that brings harmful effects which threaten single individuals, groups, states or even the entire planet, like it is for instance the case during a pandemic (Blyth 2009).

A pandemic is a special kind of crisis whose negative impact on society and business is immense. However, there is are further events an organisation threatens, like for instance an incident which represents an event whose result is an interruption of business operations, like for instance a failure of service quality. The severity of incidents plays an important role in this context (Swissbanking 2013).

2.2. Severity of Incidents

The severity of incidents is of high importance because each incident level leads to different consequences. Hence, the degree of severity has to be calculated at first. Figure 1 shows the three stages regarding the severity of events: Incident, major incident and crisis (Swissbanking 2013).

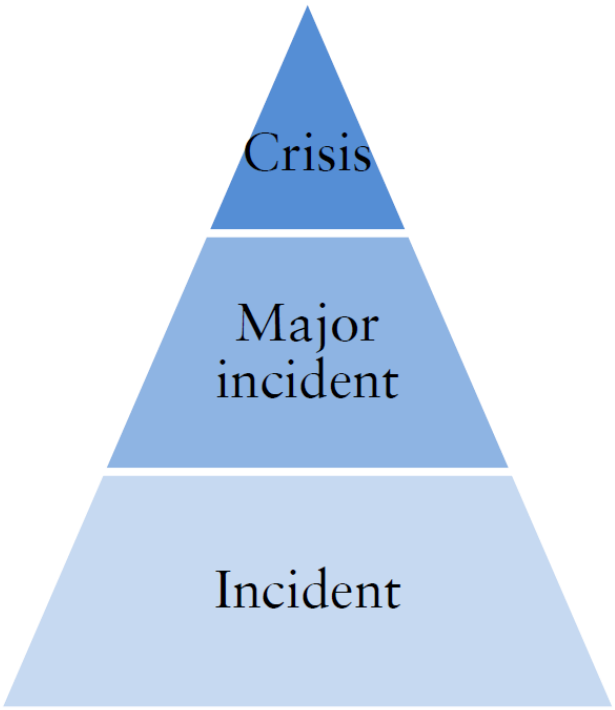


Figure 1: Severity of Events (Swissbanking 2013:18)

By taking a closer look at Figure 1, it becomes obvious that incidents show a higher frequency regarding their occurrence than a crisis. The reason for that, is basically that incidents occur more often in organisations. It is noted that an incident managed badly may lead to a major incident (second level of the pyramid) or even to a crisis in succession. However, there is no guarantee on this chronology because a crisis may emerge by itself, without a certain incident that arose before. The following paragraph will provide an overview of specific severities of events that an organisation may face and deal with.

An incident cannot be specified closer, shortly after its occurrence. A major incident is seen as a sequence of more than one incident arising which in total leads to the occurrence of a bigger event. The top of the pyramid is symbolized by a crisis which represents an extensive event of loss. A crisis represents a situation that definitely requires a specific management team that takes critical decisions in advance. The event of a crisis ranks among the exceptional events that happen to an organisation and therefore cannot be handled by the original management board (Swissbanking 2013).

According to BSI (200-4) one can distinguish between an incident, an emergency and a crisis. An incident is a kind of situation in which a certain process or a resource is not available as expected. It categorizes the lowest stage of a hazard level and the dilemma is usually recoverable besides the usual mode of operation. If incidents are not taken seriously enough which means that no actions or measures are taken to offset the prejudice, the possibility of an incident becoming an emergency does still exist. An emergency is a special kind of incident that is considered more serious and usually stands for a significant interruption or even a shutdown of critical business operations. Especially in this kind of situation an organisation applies its emergency plans that have been previously finished. The worst situation for an organisation is a crisis. It stands for a massive interruption of business-critical processes and poses a huge challenge for the organisation resting upon the fact that there are no disaster recovery plans that could be somehow applied (BSI Standard 2020, BC 200-4).

2.3. Crisis Management

Based on the unexpected occurrence of a crisis, there is a high level of uncertainty within organisations. Crisis management plays in this context an essential role as its objective is to handle a crisis effectively and in a timely manner. During an incident the so-called crisis management team takes over control and all responsibilities are transferred to them. They now have the obligation to manage all further business operations until the normal operation mode is reached or restored again (Swissbanking 2013). According to Herbane (2010) crisis management theory strives to develop action plans for situations in which the normal mode of operation gets interrupted. In this context the management method Business Continuity Management (BCM) is of particular significance (Herbane 2010).

> *"Company-wide management approach (policies and standards) designed to ensure that business-critical processes can be maintained or restored as quickly as possible in the event of (internal or external) incidents. BCM therefore encompasses the planning, implementation and controlling phases and covers the entire associated environment (areas, processes, technologies) required to ensure that, following an incident, businesses-critical processes are continued without interruption recovered within a defined timeframe"*(Swissbanking 2013)

The theory of BCM will be separately presented in chapter 4 of the present thesis.

However, a crisis is characterized by high uncertainty, there are possibilities for an organisation to make preparations for this kind of scenario. Business Continuity Management for instance represents an option to tackle the issue crisis. Figure 2 shows the course of an incident in a company.

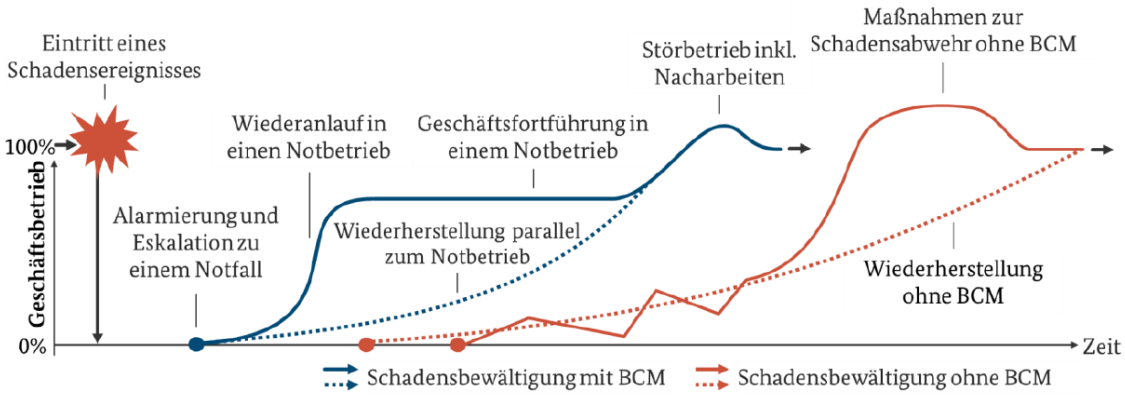


Figure 2: Procedure of an Incident (BSI Standard 2020, BC 200-4)

While the x-axis illustrates time, the y-axis shows the ongoing business operations as a percentage. The red line represents a company without an implemented BCM-system and the blue line illustrates an organisation which has a BCM-system already included to their business operations. It becomes visible that the altering system sounds the alarm way earlier in the case a BCM-system is implemented to a business. Furthermore, it becomes visible that the consequences of an incident without a prior implementation of a BCM-system are worse to the organisations. Especially, the differences regarding the altering system brings severe effects to the organisation. Time is costly which implies that the longer a process fails, the longer a subsequent process needs for restarting. This downtime means enormous cost and fatal consequences (BSI Standard 2020, BC 200-4).

Figure 2 clearly points out how relevant the study of BCM for organisations, institutions, corporations and businesses of the 21st century is. Therefore, the relevance of BCM is uncontroversial as figure *Procedure of an Incident* explicitly illustrates (Folkers 2017).

The significance of BCM is based on a complex micro- and macro environment that is rapidly changing and the accompanying threats an organisation has to deal with. Besides, the emergence of new crisis plays a relevant role as well. Covid-19 for instance represents a new kind of a pandemic that societies and businesses all over the world have to deal with. Basically, a pandemic considers a special scenario of a crisis that is characterized by high seriousness. However, there is a difference between a crisis and a pandemic regarding the planning process.

2.4. The Difference between a Crisis and the special Scenario of a Pandemic

BCM deals with crisis-scenarios. However, someone has to distinguish between BCM-crisis-planning and pandemic planning as those two differ concerning the duration and the dimension of the outbreaks can be foreseen (Swissbanking 2013).

While, a pandemic is like a crisis an unexpected situation that comes in line with high uncertainty (Blyth 2009), a pandemic differs in the following sense:

A pandemic is a worldwide epidemic. An influenza pandemic is caused by a novel influenza virus that is capable of causing severe illness and spreading well from person to person. Since this new pathogen has not been present in the human population before, or not for a very long time, the immune system is not prepared and therefore not protected.[2]

The main difference between a crisis and a pandemic is related to the time period. A crisis arises immediately and has kind of an unpredictable character. Its consequences are fatal for society and entire business procedures and its effects could reach all levels of an organisation. Regarding the recovery time of a crisis, the most important aspect is the resumption of relevant operating business tasks. By contrast, a pandemic has an even longer time horizon. While a crisis suddenly arises and stays for a certain, mostly shorter period of time, a pandemic arises abrupt as well, but usually lasts for an unexpected, longer lapse of time. For this reason, the creation of a specific pandemic plan is strongly recommended for an organisation (Swissbanking 2013).

Covid-19 represents one of the major pandemics in human history (Simmank 2020). At the outbreak of Covid-19 lives of people all over the globe changed drastically. Besides, businesses of all kinds have also been faced with extreme challenges. From an organisation´s perspective BCM became more and more significant because business operations needed to be continued even under extraordinary circumstances. Particularly critical infrastructure organisations have been especially affected.

The BCM-divisions of Deutsche Bahn, Austrian Red Cross and German Patent and Trade Mark Office had to deal with various challenges concerning Covid-19. Those will be briefly presented within the following paragraphs.

At DB the BCM division is indispensable regarding the tasks concerning the coverage of the Covid-19 pandemic. The department actually has taken on an important role since the outbreak of the pandemic because it is acting as kind of crisis manager. Their main task was to pass on a certain amount of information input to the departments in order to guarantee them more confidence regarding the handling security in managing the pandemic. During the first months of the pandemic Covid-19, the greatest challenge for DB actually was the absence of their clients. Due to the risk of contracting the virus, people in general tried to avoid the usage of all kind of public transportation as much as possible. In particular, for DB this implied that their supply regarding for instance the seating capacities was not fully stretched at all.

Since the outbreak of the pandemic, various working groups have been established at DB. They monitor the situation or coordinate and control concrete measures on a regularly basis. The pandemic plan was redrafted and adapted to the current circumstances together with the specific departments. In this context, the allocation of staff resources was one of the biggest challenges for DB. Priorly to the outbreak of Covid-19, the subject of personnel resources has been separately highlighted in the hazard catalogue provided by the Federal Office for Information Security (BSI). A result of the discrete catalogue implementation was that staff resources have been newly evaluated. In this sense, the department deals with human resource planning, specifically with the capacity planning of personnel at a particular location X at a certain time Y.

At the German Patent and Trade Mark Office requests for the protection of spiritual property have slightly decreased since the pandemic broke out. A reason for this is seen in lower production based on the lockdowns that took place. However, there were also areas, such as the trade mark area, where brand applications increased during the crisis.

[2] https://www.rki.de/SharedDocs/FAQ/Pandemie/FAQ18.html

Besides, it has been found that employee's cooperation is handled effectively even if there is more physical distance between team members. As a result, the regulations regarding the number of employees having the permission to work home-based increased. The pandemic management mainly falls into the responsibilities of the emergency management. In this context, tasks of the emergency management were for instance the procurement of home-office equipment and regulations concerning the number of employees which is acceptable in one office room. Since the quota of part-time jobs at the DPMA is very high, it has been relatively easy to handle the number of employees that are physically in the office at the same time.

While the German critical infrastructure organisations made an important contribution to the crisis management of their respective businesses, Austrian Red Cross was as well significantly involved in managing the crisis in Austria. Within media Austrian Red Cross has often been presented as staff field considered as kind of advisor of the federal government (Unknown 2021).

Before the outbreak of Covid-19, there were already prefabricated BC-plans concerning the threat of a pandemic, but only those for an influenza that were not one-to-one applicable. Due to Covid-19, the Vienna Red Cross has developed an operational command staff that deals with the topic of general disaster management behaviour. For instance, they develop measures in the area of hygiene behaviour. A separate competence centre that deals with security concepts for events in consideration of Covid-19 has been established in Vienna as well. They are dealing with issues like flows of people and strive to develop procedures concerning the avoidance of large gatherings of people.

In the area of BCM, corporate crisis staff has been established nationwide throughout Austria. An internal organisational unit and a special BCM task force for the Covid-19 crisis management has been particularly set up. Among other things, the task force dealt with topics like for example the procurement of required protective equipment that employees needed in their offices.

The previous paragraphs show that the BCM divisions have been strongly challenged since the beginning of the Covid-19 crisis and have taken on many coordination tasks. One motivation of the present thesis is to demonstrate the BCM-systems that are currently in-use at Deutsche Bahn, German Patent and Trade Mark Office and Austrian Red Cross. The following chapter will therefore illustrate the BCM-system of the three critical infrastructure organisations.

However, a brief digression has to be made before on the subject of critical infrastructures and their regulations in Austria and Germany. This should contribute to a better understanding of the reader regarding the subject critical infrastructures.

Critical Infrastructure Organisations – A brief Introduction

An organisation´s system that is of high significant for maintaining vital economic and social functions is understood as a critical infrastructure organisation. Those functions consist of various components, like for instance health, security, food, energy, etc. (European Commission 2021)[3]

Critical infrastructures are not bounded by national borders and mostly interacting across multiple countries. This fact implies that for the long-term success regarding the protection of critical infrastructures, an excellent cooperation between the individual countries is considered as a basic prerequisite. In this context, there are various guidelines provided, for instance the one by the European Union (Willisegger 2018).

The threat of a blackout for instance has brought new challenges for critical institutions over the last years. Voices that warn of negative developments and potential failures are getting louder and louder. Based on the increase of information and communication technologies, the micro- and macroenvironment regarding the exchange of information within critical infrastructure organisations changed. A failure in one area can have fatal consequences for many linked areas. Therefore, the systemic view plays a central role (Saurugg & Pichlmayr 2013).

Based on the following qualitative analysis and the results which have been examined by the expert interviews conducted with Deutsche Bahn, the German Patent and Trade Mark Office (DPMA) and Austrian Red Cross the following paragraph will exclusively present a brief overview concerning the management of critical infrastructures in Austria and Germany.

Situation in Austria

During the last years the importance of protecting critical infrastructures continuously grows. This is due to various facts, like for instance the increasing number of cyber-attacks. In Austria the national program for the protection of critical infrastructures has been released in 2008. Based on the guidelines developed, there has been a revision in 2014 and a new Masterplan has been published.

"APCIP Master Plan for the reliability of supply in food, transport, telecommunications, energy and financial services, as well as social- and health services."[4]

The plan is based upon cooperation, subsidiarity, confidentiality and other principles and aims to support companies that are of high significance from a strategical point of view for the Austrian community. (Bundeskanzleramt Österreich 2016 cited from: Hunziker & Meissner 2017).

[3] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12462-Protecting-critical-infrastructure-in-the-EU-new-rules_en

4 https://www.bundeskanzleramt.gv.at/themen/sicherheitspolitik/schutz-kritischer-infrastrukturen.html

Situation in Germany

In Germany the management of critical infrastructures falls into the responsibility of the public authorities, especially into the one of the German ministry of the interior. For the proper functioning and the protection of critical infrastructures, Germany has developed the so-called “Nationaler Plan zum Schutz der Informationsinfrastrukturen” and a following “Umsetzungsplan KRITIS”. The plan covers guidelines for the protection of critical infrastructures developed in a joint elaboration between governmental authorities on the one side and 30 infrastructure operators on the other side (Bundesministerium des Inneren 2007 citem from: Hunziker & Meissner 2017).

CHAPTER III.

Qualitative Analysis: Expert Interviews

The following chapter constitutes the empirical component of the thesis.

A qualitative analysis in the form of expert interviews has been conducted with Deutsche Bahn (DB), the German Patent and Trade Mark Office (DPMA) and Austrian Red Cross.

The following chapter illustrates the differences between the individual BCM-systems and shows the properties of each individual BCM-system. In this context, drivers for BCM, BCM developments, BCM process, responsibilities-, tasks-, threats- and objectives of BCM, as well as needs of the current BCM-systems and expectations for further improvements are described.

The chapter concludes with a table that summarizes the characteristics of the individual BCM-Systems.

3.1. Expert-Interview I.: Deutsche Bahn

April. 22nd 2021
Angelika Oswald & Patrick Theuer
Corporate Security (IZ)
Business Continuity Management

Brief organisation overview
Deutsche Bahn (DB) is one of the world's leading providers regarding mobility and logistics. The critical infrastructure company employs over 330,000 people worldwide, more than 210,000 of them are situated in Germany.
Besides the areas of traditional railway infrastructure, the company specifically deals with the research and the operation of transport networks in future days. Therefore, a main focus of DB is to connect the attributes of an economically and ecologically mode of transportation for future days. (Deutsche Bahn 2021)
As DB represents one of the main critical infrastructure organisations in Germany, the responsibilities for guaranteeing the security of supplies are set high. The guarantees cover a broad area, from terrorism to power supply systems. (Deutsche Bahn 2021)

3.1.1. BCM Developments

Since the huge cyber-attack `WannaCry´ took place in 2017, the developments of an individual BCM division at DB began.
According to estimations, which were conducted by the IT-Security company Avast, more than 45,000 single attacks were performed. The huge cyber-attack, which brought international fatal results in 99 countries, especially for Russia, the Ukraine and Taiwan, even affected Deutsche Bahn. The results of the Trojan attacks were system failures and downtimes as well as whole breakdowns or error messages concerning digital scoreboards (Frankfurter Allgemeine 2017).

At DB, `WannaCry´ is seen as one of the main triggers for a greater significance and general meaning of business continuity. Besides, the cyber-attack is a main driver regarding the establishment of an individual BCM division at DB. After `WannaCry´ was completed, a board resolution followed which determined the implementation of a holistic and group-wide BCM division that should be ISO-based. The aim was to ensure the continuation of critical business processes in the event of damage or crisis. In more detail, this stands for an explicit analysis of potential damages and dependencies, the definition of requirements and resources for critical processes as well as the development and implementation of strategies and business plans.
The BCM implementation process at DB started in 2018 and is still under development in 2021. The achievements of the development process were built on three stages: the definitions of the BCM-specifications, the embedding process, for instance the position of the BC-manager and finally, the implementation process which covers the conducted BCM-process-cycle and the shift to the operating phase.

Important to note in the context of BCM-developments at DB is their connection to the IT Safety Act / KRITIS which covers all covers all system-critical infrastructure organisations that are relevant for the reliability of supply throughout Germany. This implies that DB is bounded by regulations of the BSI (Federal Office for Information Security).

3.1.2. BCM at DB

At DB Group BCM is centrally embedded in the Group Security division.

Generally, BCM at DB is divided into two areas. The first area is the emergency planning, which is based on the development of preventive measures that are elaborated by the BCM-division. The second field deals with the issue of reactive actions which implies that the focus lies more in the field of emergency management.

In 2021 the central BCM-division consists of four persons. While the central team, located at DB Group consists of these four persons, there are over 15 additional employees that are working within the specific business areas. For ensuring that all business areas are reached and business-critical processes are comprehensively met, each business area has one BC-manager, who manages all of the cases and is responsible for the ongoing operations. Larger business areas even have two BC-managers.

The responsibilities of BCM are shared among the BCM participants, like for instance the BC-Managers or and the BCM representatives. The following table summarizes the main responsibilities of the BCM division at DB.

Strategy Development	**Conduct of Analysis**	**Provision of Validations**

The BCM-division at DB is mainly responsible for the strategy development, the conduct of analysis and the provision of validations. In particular, the division often deals with the application of already pre-developed BCM-strategies. For example, in the case of the BCM-implementation process at a specific department, certain analyses are conducted that aim to identify critical processes and their corresponding resources. In this context, there are already prefabricated plans. This implies that not all strategies and procedures have to be developed from scratch. There are existing emergency management plans that can be resorted and are applied under the right circumstances.

For ensuring that the developed BC-plans cover all relevant issues and procedures that have to be conducted in the case of an incident, the BCM division is working hand-in-hand with the risk division of DB, while both divisions are still structured separately.

In addition to different areas of responsibility, the BCM division also has different tasks to perform.

3.1.3. BCM-Process

The BCM-processes covers different tasks that need to be carried out.
Mostly, the BCM division at DB plans and develops BC-strategies on a central level that are afterwards implemented to specific business areas on a decentralised level. Group-wide in this sense means that all resources of critical business areas and service units that include critical processes are identified according to uniform standards.

Someone has to distinguish between tasks during the normal mode of operation of the BCM-division and those during times of crisis.
The first covers for instance the development of specific BC-plans which are related to tasks of the BCM-Lifecycle. This consists of the preparations of business impact analysis and risk assessments of business-critical processes, their corresponding resources and the related threatening consequences during a breakdown.

During times of crisis, BC plans and strategies are implemented and activated in order to be able to continue critical business processes during an incident.

3.1.4. BCM in the Context of Risk Management

At DB BCM fits into the existing risk security crisis and emergency management.

Risk management consists of the identification of potential threats and their subsequent evaluations. The main task of the risk management is the decision-making process concerning the risk treatment. The objective is always to minimize the level of danger and the probability of risk-occurrence, to deal with the risk acceptance and the prevention as well as the transfer of risk. BCM has already been dealt with in Risk Management before the actual implementation process even started in 2017. In this context, the development of measures for counteracting preventive as well as reactive scenarios were already part of the risk and security management. The process was characterized by an easy approach where risks have been identified and measures have been initiated for dealing with them.
Once a damaging event or an incident has occurred, the emergency response activities were commenced by the crisis management and the emergency management started with its operations. The activities consist of the report, the escalation, the following situation report, the evaluation, the crisis communication and the crisis response. Emergency management is practiced and trained preventively in emergency planning in order to be best prepared for the case of an emergency.

The missing key before a sustainable BCM-system has been implemented, was the lack of identification of business-critical processes, those which were particularly worth protecting.

This is an important aspect regarding the long-term success of BCM at DB. Strategies and plans for the failure of critical operations are created, implemented and tested. For this purpose, information and data of significant processes is provided by the risk management and plans regarding the continuation are developed. In the following step, these roadmaps are forwarded to the decision-makers in crisis and emergency management, so that they can be applied in the case of an incident. The ambition is that damages can be assessed quickly and repaired in an adequate manner so that further processes are affected as little as possible.

3.1.5. Threats

The main dangers of BCM are primarily seen in external factors.

Due to digitalisation and the main threats are seen in the scenario of cyber-crime, like for instance the huge cyber-attack WannaCry in 2017 that also affected DB, the occurrence of blackouts, and terrorism.

<u>The scenario of a blackout at DB</u>
The risk of a blackout is a deliberate risk factor at DB Group. Particularly in the driving operations, a power blackout represents immediate consequences and severe impairments. Even small power failures, even only at a regional level, can lead to massive impairments and disruptions.
Even though sufficient preparations regarding this scenario have been already made at DB, like for instance the purchase of emergency power generators or diesel-powered motor vehicles, the status quo shows that one is limited and poorly equipped for an emergency situation. One of the main problems in the event of a power blackout is the busy grid, as the track is occupied by trains that simply come to a standstill.
In this sense, on the one side a blackout is considered a main threat, on the other side BCM contributes an essential input concerning the development of blackout-countermeasures.

3.1.6. Objectives of BCM

The main focus lies in the identification of business-critical processes and the establishment of a holistic and group-wide BCM-system for the continuation of those and the recording of their corresponding critical resources. Resources include IT, buildings, infrastructures and means of production, deliveries, service providers, construction works as well as personnel located in the certain processes. The critical processes should be identified within each business segment according to uniform and comparable standards.

Further aims of the BCM-Division are the identification of BCM-relevant topics throughout DB Group. Besides a BCM-strategy should be established and damage potentials and failure risks are analysed and incorporated to the strategy developments. Finally, requirements for the conducted trainings and performing exercises are set.

3.1.7. Expectations/Need of the present BCM-Systems

Currently the issue of system overload based on high volumes of data is remarked by Deutsche Bahn. Data volume got too big and complex to deal with. The BCM-division of DB is mostly working by the application of excel sheets. As an outcome, systems reached their limits. Additionally, the high volumes and high speed of data leads to slowed process flows within the systems.

The DB BCM-division´s ambition is therefore to find a tool that facilitates and optimizes the workflow. In more detail the expectation is that information should be easily retrievable by just a few clicks. A feature of the queried information is that they are always up-to-date and pre-evaluated or rather validated. Furthermore, the possibility to insert relevant data to the tool should be given to all departments that are involved in the same working steps or project.

Besides, DB expressed a high demand after a tool that automatically implements critical processes of different departments and disciplines into their BCM-system.
At the moment the BCM-division at DB has to fulfil this step on their own. This means that the critical resources of the individual departments have to be discussed with the respective divisions, before implementing them to the BCM-system. This is an extremely time-consuming process and requires a lot of personnel resources especially regarding the cataloguing. Therefore, it would be much easier and more helpful if there was a central system and database that everyone could access collectively.
The status quo at DB is that the current tasks are done by the usage of Excel templates. This turns out to be extremely tedious and time-consuming, as the data is getting bigger and bigger and the overall view is lost. Additionally, data became too complex. As one result, various error messages characterize the current condition.

To sum up, the BCM-division at DB sees itself more as kind of a documentation management- and general reference system, that collects all of the BCM-relevant information and subsequently integrates those into a plan. The BCM process at DB is characterized by a traditional BCM-approach as many common-known BCM-tools are applied like for instance the Business Impact Analyses (BIA) which is applied for the further establishment of a BC-plan. One of the main challenges of the BCM-systems at DB is related to the object database that is currently in-use is. Due to the huge amount of data, processes got slow and inefficient.

3.2. Expert-Interview II.:

German Patent and Trade Mark Office /
Deutsches Patent- und Markenamt (DPMA)

May, 5th 2021
Annette Kirchner
Head of Strategic Process Management (Stabstelle 0.3)

Brief organisation overview
The German Patent and Trade Mark Office is the central contact point and the centre of competence for industrial property protection in Germany. Their main task is the protection of intellectual property. The fifth largest national patent and trade mark office in Europe employs more than 2,500 employees which are allocated among their offices in Berlin, Munich and Jena. (DPMA 2021)

3.2.1. BCM Developments

BCM has been developed in parallel to the already existing emergency management. DPMA made the initial steps of the BCM-implementation in 2018 and is currently still in the development phase.

Besides, the DPMA is currently in the process of becoming more process-oriented. For this purpose, a process portal has been developed, which is used to publish valid processes. The individual management instruments are brought together via these processes. For example, the strategic goals are linked to the processes in order to illustrate which processes contribute to strategy implementation, independent of the measures that may still be changed. The strategic and operational goals are derived from this procedure.

In 2011, a fully electronic file processing system was introduced, which has since then been used by all divisions, like for instance the protection-, legal area-, patents- and utility models- department. Therefore, paper files no longer exist. Everything was digitised and then packed into a digitised workflow.

The DPMA primarily has a statutory mandate to fulfil. The public administration has the duty to fulfil its legal mandate. This implies, that based on their close association with public authorities the DPMA strongly has to adhere to the guidelines of the Federal Office for Information Security (BSI).

The time target for BCM implementation was initially set until the end of 2022. However, since difficulties arose already at the beginning of the BIA conduction, the completion process is delayed.

The next steps that need to be conducted are the completion of the BCM implementation process. It is understood that the system should be a cross-departmental one. However, it is not yet known where the BCM department will be centrally located at the DPMA.

3.2.2. BCM at German Patent and Trade Mark Office

In general, DPMA understands as BCM the readiness and well-preparedness in the case of an incident or an emergency. Furthermore, this implies to be well-prepared for the organisation itself and that business-critical processes could be restarted quickly.

The DPMA has a certain IT emergency management system consisting of a -guideline, a -preparedness concept, -plans and -manuals. In addition, there is a strategic and operational process management and a process map, that covers all business processes of the German Patent and Trade Mark Office. Basically, the dealing with risks mostly falls within the remit of the IT emergency management system.

The aim of business continuity management at DPMA is to identify the critical processes and resources that still have to be available in an emergency situation or during a crisis. Besides, it is about the actual development of an emergency management system.

However, the issue of business continuity is taken serious throughout the entire organisation, there is no independent BCM-division so far. Basically, BCM is part of many different departments, like for instance the strategic process management. Other departments that are taking place in the implementation process of BCM are for instance Data Protection, IT and Organisation, IT Emergency Management, Information Department and Human Resources.

3.2.3. BCM Process

At DPMA, the BCM process starts with the identification of critical processes and their related business endangering risks.

This step is followed by a BIA in which the criticality is assessed and maximum tolerable downtimes are calculated. In more detail, the focus lies on the identification of the corresponding resources to the business system critical processes.

At the third stage a risk analysis is conducted which identifies the hazards that could cause an interruption of certain processes –naturally all in line with the standards provided by the BSI. At the moment BCM at DPMA is executing this risk analysis (risk matrix). In the course of this, the DPMA wants to place the process at the centre and accordingly attach the risks to the processes. Besides, they strive to establish a specific risk management division at the DPMA.

Finally, continuity strategies are developed and an emergency manual or emergency preparedness concept is created.

After the evaluation phase, the results of the BIA will be directly incorporated into the process management.

3.2.4. Threats

Based on the DPMA´s statutory mandate to fulfil and their administrative principle, the financial loss in risk evaluations, which is usually a threat taken seriously by companies does not exist. In addition, there are also no direct competitors. Dangers lie more in the area of time management of orders. This means, for example, that a patent is not approved in a certain period of time, or until the original deadline. As a result; the patent applicant suffers a financial loss. Besides, a serious risk for the DPMA is for example, an infrastructure failure in Germany, like for instance the scenario of a blackout or the issue of cybercrime.

3.2.5. Objectives

In general, the public administration´s success is strongly related to the success of the BCM system.

By implementing a BCM-system to the DPMA; the expectations are that processes are accelerated and tasks are allocated more efficiently. Besides, responsibilities should be defined more precisely and all factors together should contribute to an even better outcome and holistic success of the DPMA.

3.2.6. Expectations/Need of the present BCM-Systems

At DPMA, the main expectations for an improved BCM-system are that processes are accelerated and tasks are distributed in a more efficient way. DPMA could imagine to implement a further tool that supports the present BCM-systems. However, the implementation of such a tool should be in line with the functional organisational structure. This implies that the responsibilities of the individual departments are precisely set within the administrative area.

To sum up, DPMA considers BCM the readiness and well-preparedness in the case of an incident or an emergency. The BCM implementation process at German Patent and Trade Mark Office started by the identification of business-critical resources and their related risk in the case of a failure. Subsequently, continuity strategies are developed according to the risks identified, and finally an emergency preparedness concept is drawn up. Important to consider at DPMA is that it has a statutory mandate to fulfill. This implies, that DPMA has to adhere to the guidelines of the Federal Office for Information Security (BSI).

3.3. Expert-Interview III.: Austrian Red Cross

June, 25th 2021
Michael Sartori
Landesrettungskommandant Wiener Rotes Kreuz
Member of the Executive Board at Wiener Rotes Kreuz

Brief organisation overview
Red Cross is an international non-profit organisation that is operating in the fields of aid delivery, emergency services, disaster preparedness, disaster relief, integration, development cooperation, blood donor services, health and social services, search services, humanitarian international law and international aid. In Austria the organisation employs more than 8,000 people and counts more than 72,000 voluntary members. (Rotes Kreuz 2021)

3.3.1. BCM at Austrian Red Cross

Based on the organisation´s 50+ years of experience in disaster management, the approach of BCM is part of the NGO´s DNA. Therefore, there is no individual BCM department, and the issue is spread all over the organisation.

BCM at Austrian Red Cross is primarily understood as the contribution to the common good. BCM deals with all organisational units and field of activities, like for instance raw materials supply, emergency services, civil protection, social services and care and support services.

In the area of care and support the main challenge is to ensure that nursing staff is always available. In the case, that the number of care-staff is too low, could bring disastrous consequences to many persons who are in need of nursing. This scenario shows a situation in which business continuity at Austrian Red Cross comes into play.

Basically, Red Cross understands under the term business continuity the specification of the kind of business or operating areas that have to be available on a permanent basis, especially in the case of a crisis or an incident. For instance, the emergency service has to be available anytime and the rescue services have to be guaranteed on a permanent basis.

However, BCM is understood as major part of the organisation´s philosophy, there is no certain BCM department at Austrian Red Cross. Based on the heterogeneous organisational structure, BCM is embedded in the regional association as well as in the secretariat-general (the holding) in Vienna. Besides, the differences among the federal states enable a close working relationship with the individual legal entities, public authorities and the politics of the federal provinces.

Being in a regular exchange with the authorities of the federal states and other important players is considered to be the basic prerequisite for the proper functioning regarding disaster management and BCM. The only difference between the two disciplines is the number of people involved in disaster or incident management.

Based on the organisation´s field of operations, like for instance the emergency services, disaster preparedness or the disaster relief Austrian Red Cross presents itself as an agile and flexible organisation regarding its dealing with the situation of any crisis.

The Austrian Red Cross is thus seen as kind of a key player in Austria in managing crises and disasters together with politics, public authorities, legal entities and further institutions.

3.3.2. BCM Process

As most of Austrian Red Cross services are system-critical, their BCM deals a lot with the evaluation of risks and the set of priorities concerning their most critical services. Questions such as the threshold value of acceptable risk, the establishment of special defence measures or the procedure in case of failure of critical services are analysed in detail.

In general, precautionary measures are developed for issues like for instance the identification of threats, the procedure of counteracting measures, the risks which are derived from the hazard analysis, the definition of services than should be maintained at all costs as well as the services than should be still offered during times of crisis or what kind of services could be dispensed during an incident so that resources can be used in another business area.

There are prefabricated BC plans that can be easily applied in the event of a disaster or incident.

The application of a risk matrix is at the moment only in use at the state association in lower Austria, where a single person is currently responsible for the issue of BCM. Subsequently, the hazard levels could be read off.

Traditional BCM-tools, like for example the business impact analysis are currently not in-use, however the plan is to introduce those kind of traditional BCM-tools and procedures in the future for the creation of standardized processes. The thesis will go into more detail concerning BCM-tools in the following chapter.

3.3.3. Threats

Threats that the Red Cross is currently dealing with in the field of BCM are natural disasters (floods) based on climate change, terrorism, blackouts, etc. The main concerns in this area are interrupted communication channels, i.e., a disruption or a failure of the Wireless Broadband connection. This issue is highly-relevant due to the fact that indeed all Red Cross operational systems are based on the principle of flawless communication.

Besides, Red Cross is additionally dealing with the issue of intentional threats. Nationwide, there is a good cooperation between the individual authorities, the Red Cross and other relevant Austrian institutions, especially those which are operating in the field of disaster management. Especially in disaster control, an international peak is remarked, like for instance regarding the scenario of an occurring blackout.

In the event of a blackout, a solid basis of plans is already established that could be applied. It is important to note that a certain amount of improvisation is always required in the event of a disaster. This implies that prefabricated BC-plans cannot be applied one-to-one. For a certain blackout-scenario, special BC plans have already been developed together with the municipal administration situated in Vienna. Though, the BC-blackout-plan has been solely developed for the scenario in the capital of Austria. The reason for this is based on the sometimes-challenging situation in Austria due to the federalist concept.

In the forum of the provincial rescue commanders, a kind of supra-regional exchange takes place between the individual provincial associations. In this context, a lot of exchange has been recently invested in the field of blackout prevention.

In general, there are plans for different potential scenarios. In the event that there is no concrete plan of action for an event, one knows how responsibilities are distributed across the federal government and to which authority, institution one must turn.

3.3.4. Objectives

The main objective of BCM at Austrian Red Cross is the creation of awareness concerning the issue of BCM through the entire organisation. Besides, the aim is to be best prepared against the occurrence of the potential threats identified. A further objective is to standardize processes in the future. In this context, the application of traditional BCM-tools, like for instance the BIA should be implemented to the BCM-process.

3.3.5. Expectations/Need of the present BCM-Systems

Austrian Red Cross definitely recognized an improvement considering the paradigm shift. There is a big demand after a tool that improves the business continuity activities. As the plan is to greatly expand a division that is particularly responsible for BCM at Austrian Red Cross, it is definitely desirable to implement a further tool that supports the BCM-systems. Besides expectations are for instance that processes are visualized and critical processes and resources are always highlighted separately.

To sum up Austrian Red Cross is seen as kind of a key player in Austria concerning crises and disaster management. Therefore, the NGO considers BCM part of their organisation´s DNA. There is a strong need that a further tool is implemented to the BCM-system for increasing its effectiveness. In this sense, also the topic of awareness creation is important because it is relevant to make employees aware of the BCM-issue because BCM is considered under a latent threat.

Comparative Analysis

As a result of the expert interviews, the following table has been developed that summarizes the main characteristics of the BCM-systems of Deutsche Bahn, German Patent and Trade Mark Office and Austrian Red Cross.

The table shows the features of the individual BCM-systems and furthermore highlights their common attributes and differences.

Characteristics BCM-Systems

	Deutsche Bahn	**Austrian Red Cross**	**German Patent and Trade Mark Office**
Start of development	2018	over the last years	2018
Structure	division centrally located within the Group	throughout the organisation --> embedded in the organisation´s philosophy / due to heterogenous structure BCM in regional associations as well as in the secretariat-general	cross-departmental, not sure yet if final division will be centrally located
Responsibilities	strategy development, conducting analysis, provision of validations	continuation of aid delivery and emergency service (e.g., care and support)	strategy development and plans of action for times of crisis
Threats	cyber-crime, blackout, terrorism	blackout, pandemics, natural disasters (climate change)	Blackout, cyber-attacks, order delays (patent applicant suffers financial loss due to not completed approval procedure during a certain period of time)
Objectives	identification of business-critical processes and corresponding resources / identification of BCM-relevant topics for entire DB Group	creation of awareness through entire organisation / excellent preparation for any of the potential threats identified	fulfilment of statutory mandate / optimal preparation for any crisis scenario / identification of business-critical processes
Products generated	development of BC-strategies on a central level	development of BC-plans that can be easily adapted and applied to different kind of scenarios	development of continuity strategies / creation of emergency manuals or emergency preparedness concepts

Tasks	typical tasks and tools of the BCM-lifecycle, "Vorscoping", BIA, RIA, …	development of BC-plans, by identifying critical processes and services that need to be available under any circumstances	typical BCM-tools like e.g. BIA
Evaluation of risks	risk matrix	status quo: risk matrix only used in lower AT, otherwise individual risk assessment	risk matrix
Decision-making-process	always according to the risk level	based on BC-plans / in cooperation with experts of institutions, federal government, state associations, …	not yet finalized/known
Need	tool that: deals with huge amount of data / optimizes overloaded systems / enables access privileges for more participants from various divisions / optimizes standardized and faster decision-making process	tool that: manages the entire BCM process holistically and consistently throughout the organisation	tool that: optimizes the decision-making process in a later stage of BCM implementation

The table summarizes the features of the single BCM-systems of the organisations interviewed.

It shows that the individual stages of the implementation process differ. As Deutsche Bahn is quite progressive regarding their already established BC-plans, DPMA and Austrian Red Cross are at an earlier implementation stage. However, one characteristic that all three critical infrastructures have in common is that they all haven´t finished the entire implementation process so far.

Beyond that a further similarity is seen in the connection of the tasks by the emergency management and the individual BCM-departments. All three critical infrastructure organisations show that their emergency management is strongly related to the departments that are responsible for BCM.

To sum up, the responsibilities and objectives concerning BCM look quite similar at Deutsche Bahn, DPMA and Austrian Red Cross. Their main propose is obviously being best prepared for any situation of crisis. For this reason, the products that could be seen as kind of an outcome that the BCM-divisions produce are mostly BC-plans or manuals that are applied during an incident or an unexpected incident.

The differences between the critical infrastructure organisations are mainly noticed considered their BCM-tools applied. While DB is fulfilling the entire BCM-lifecycle by applying well-known tools like for instance the Business Impact Analysis (BIA), Red Cross is only conducting a BIA in a specific state association in lower Austria.

Furthermore, the table illustrates that the main threat of all organisations interviewed is seen in the scenario of a blackout. The loss of electrical power supply is considered as an issue that needs to be taken serious as all relevant operations demand for a proper-functioning power supply system, for instance like the principle of flawless communication in the case of an emergency at Austrian Red Cross.

Finally, whether the individual BCM-systems are in a proceeded implementation stage or not, there is already a need after a tool that supports and expands the BCM-systems that are currently in-use especially regarding the issue of high amounts and high-speed of data which poses the greatest challenges to the current BCM-systems. Therefore, for ensuring future effectiveness of the BCM-systems of the critical infrastructure organisations interviewed the implementation of a further tool is definitely needed. Before the thesis deals with the issue of the implementation of a further tool for expanding the BCM-systems of DB, DPMA and Austrian Red Cross, it is necessary to analyse the theory of BCM in more detail because it contributes to the reader´s comprehension of the following tool developments.

CHAPTER IV.

Theory: Business Continuity Management

Already in the beginning of the thesis it has been stated that the term uncertainty plays an important role, why Business Continuity Management got more and more attention over the last decades. Disasters and catastrophes (from calamities of nature to financial crisis) put new challenges for critical infrastructure organisations. Businesses tackle this issue by establishing or improving their Business Continuity Management capabilities, for instance by optimizing their emergency response and crisis management. More and more organisations strive to be best prepared for the scenario of any incident, by developing specific Business Continuity Plans or Disaster Recovery catalogues (Hiles 2011).

This phenomenon has also been observed at the critical infrastructure organisations that have been interviewed for the present thesis. The developments of their BCM-systems have just started several years ago. However, all of the interview partners are currently in the process of development of their BCM-systems, the comprehension of BCM is in some sense diverse, as also BCM-theory shows.

4.1. Definition Business Continuity Management

The definitions of Business Continuity Management are broad.

On the one side, BCM is understood as kind of management tool that is applied by organisations to carry out preparations for the situation of crisis. In this context, the aim is to be best prepared during an incident and to guarantee that a business´s legal obligations are still met (Wong 2014).

On the other side, Drewitt (2013) classifies BCM as part of an organisation´s risk management that shows its core competencies in the identification of critical processes and their corresponding resources that could be interrupted by external threats, like for instance losses (Drewitt 2013).

Some definitions highlight the relevance of BCM to an organisation due to its impact concerning the competitive situation of a company. Based on the integration of BCM to an organisation´s strategic management activities, a business´s operational resiliency could increase. As a result, the critical processes and corresponding resources could recover quicker in the situation of a crisis (Wong 2009).

Therefore, BCM is considered as a fixed component of an organisation (Wong 2014).

To sum up BCM is increasingly important for critical infrastructure organisations. This is seen in the fact that BCM supports the continuation of all business-critical processes and structural organisational measures of an organisation during times of crisis and the improvement in operational resilience. The considerable uncertainty played a huge role regarding the increasing occupation with BCM. The following paragraphs will show more drivers for BCM and provides an overview of the historical development of BCM (Rössing & Baumann cited from: Hunziker & Meissner 2017).

4.2. Historical Development of BCM

Continuity has always been a central component regarding a company´s corporate governance and its long-term success. First points of contact with BCM have been made within the area of the traditional civil defence. When the towers of the World Trade Centre have been destroyed by the terror attack in 2011 September, 11th, the program of “Continuity of Government” was activated (Rössing & Baumann cited from: Hunziker & Meissner 2017).

"The Continuity of Government Readiness Conditions (COGCON) system establishes executive branch readiness levels based on possible threats to the National Capital Region. The President alone determines and issues the COGCON Level."[5]

The development of BCM can be attributed various kind of disasters. From natural phenomenon, like tsunamis, cyclones, earthquakes, floods, fires etc. to economic breakdowns and catastrophes, like the financial crisis of the years 2008 and 2009, pandemics, like Covid-19 or terrorism are all events that are somehow related to a crisis.

Reports by the United Nations International Strategy for Disaster Reduction Secretariat (UNISDR) show that the main outcomes of catastrophes and disasters are losses. These losses are extremely fatal, due to the lives lost of millions of people on the one side and on the other the side the appearing economic losses which have impacts for world economics. The immense impact of catastrophes may be seen as the main reason why the importance of BCM constantly grew over the last decades (Hiles 2011).

According to the Business Continuity Institute (BCI), 0.8% of the United Kingdom´s GDP is lost on an annual basis –or to put it in other words: the UK economy loses 11.1 billion pounds each year based on bad or insufficient BCM operations in most enterprises (Hiles 2011).

Basically, disasters are nothing uncommon, however it shows that there is only one substance to rely one which is uncertainty. Catastrophes and disasters are not predictable nor preventable. However, an organisation has the obligation to be prepared in times of any crisis (Hiles 2011).

According to Randeree et al. (2012) BCM´s origin arose in the field of Disaster Recovery Planning (DRP), which goes back to the 20th century. Actually, it emerged between the 1950ies and 1960ies. During these decades' organisations first tried to store their critical information, for instance in the form of paper copies. The actual approach of DRP was based in the United States banks industry and its aim was to save their main data centres and to protect those against potential attacks or unforeseeable events. Its main aim was therefore the protection of various computer systems, instead of whole corporations or downtimes considering business operations. The shift to a broader view, regarding the safety of protection of whole entities arose later during the 1990ies when Business Continuity Planning (BCP) replaced DRP in most businesses. The thesis deals with the issue of BCP in more detail later. However, it should be briefly noted that BCP ensures to prepare whole organisations for the scenario of incidents and to protect critical business services by avoiding downtimes (Herbane 2010).

According to Bakar et al. (2015) the first developments of BCM had their origins besides the field of DRP and the disaster and catastrophes perspectives in the military field (Bakar et al. 2015a).

Disasters and catastrophes bring different kind of risks for organisations.

4.3. Different Kind of Risks

Risks imply that organisations always have to tackle new challenges. Due to a rapidly changing micro- and macro environment those threats are variously. There are two main kind of risk that an organisation is confronted with: the known-, and the unknown risks. Known risks are for instance fire, natural hazards –like for instance floods, blackouts, etc. which are all characterized of their identifiability and

[5] https://whitehouse.gov1.info/continuity-plan/#cogcon

quantifiability. A business has the possibilities to make accurate preparations against these kinds of events in advance (Spörrer 2014).

Besides, there are risks whose consequences and effects cannot be foreseen at all. This is for example shown in the scenario of a pandemic. Those negative events which may bring fundamental troubles to organisations, national authorities or other institutions are the reason why the implementation of business continuity management is of that high significance for an organisation to survive critical times of crisis (Spörrer 2014).

For this reason, different drivers for the implementation of BCM have developed, like for instance corporate governance, governmental regularities or laws, clients, investors or other types of shareholders (Spörrer 2014). One of the objectives for driving the BCM process within an organisation is seen in the term resilience. Resilience is related to the robustness of an organisation. Furthermore, it deals with a business´s agility and flexibility of processes and their corresponding resources. BCM is considered one of the major drivers for ensuring entrepreneurial resilience (Hiles 2011).

4.4. Entrepreneurial Resilience

Due to the fact, that Business Continuity Management is one of the drivers for an organisation's robustness, it is seen as a necessary component of an organisation´s entrepreneurial resilience.

While the theory of risk management puts its focus on past occurrences, resilience engineering focuses on future happenings. Traditional risk management looks at incidents from a retrospective view, and it is aiming to create certain statements about future events by adding probabilities to them. In the contrary, resilience engineering focuses on the improvement of current processes or procedures applied. The organisation strives to be best prepared for future occurrences by targeting efforts to the enhancement of businesses agility, flexibility and ruggedness. By comparing the methods of risk management and resilience engineering it turns out that the first methodology uses past events as their basis for potential forecasts, while the second method is more focusing on the contemporary situation of an organisation.

Therefore, resilience engineering is more agile in the event of a breakdown or crisis than it shows the ability to be more flexible regarding adaptation skills (Hiles 2011).

The following figure highlights how entrepreneurial resilience could grow during the Covid-19 crisis.

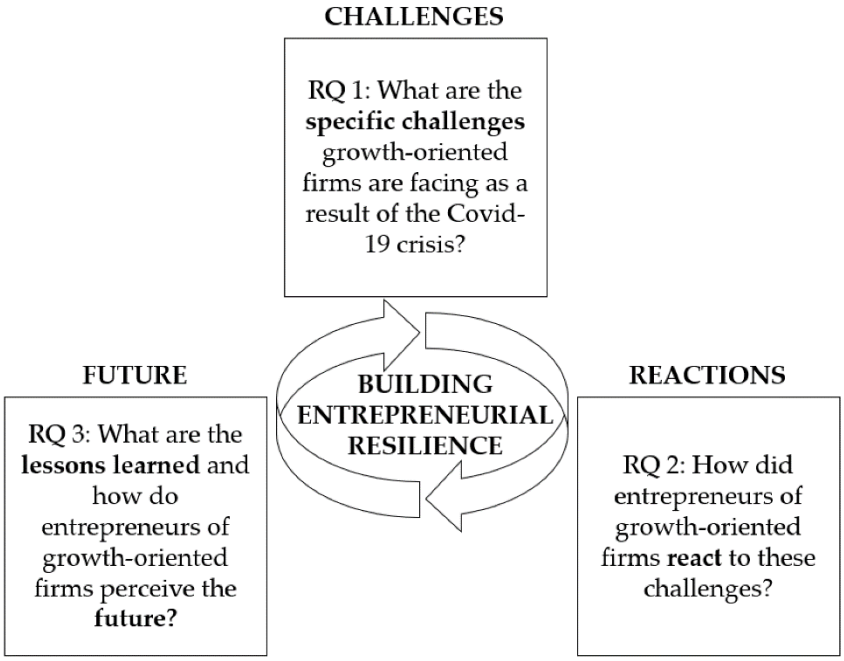


Figure 3: Building Entrepreneurial Resilience (Schepers et al. 2021)

Figure 3 illustrates how a company could gain entrepreneurial resilience during the Covid-19 pandemic. The engineering process consists of three components: *challenges*, *reactions* and *future*.

The first component (*challenges*) refers to barriers that growth-oriented companies had to deal with during the Covid-19 crisis. The behaviours of the enterprises to the challenges are presented as *reactions*. Finally, the lessons learned are represented in the third component (*future*) of the construction process of entrepreneurial resilience. In the present scenario, the knowledge gained and its impact regarding future prospects was collected during the first and second wave of the Covid-19 pandemic in Europe in 2020 (Schepers et al. 2021). In conclusion, figure 3 shows that entrepreneurial resilience and risk go hand in hand.

In most organisations BCM is part of the risk management (Hiles 2011).

4.5. BCM: Part of the Risk Management

BCM is considered a driver for an organisation´s resilience. For this reason, the division is mostly embedded into an enterprise´s risk management division. The departments are conducting different analysis regarding the evaluation of potential threats that an organisation is facing.

For instance, a risk analysis is a concept that is often applied by BCM departments. In this analysis critical resources, like processes or company´s assets that are particularly worth protecting are identified. The components that have been identified, play a huge role regarding the cause of a damage. Additionally, they represent potential threats, that could lead the organisation towards an incident or interruption within the production process.

The main goal is definitely not to highlight all of the potential threats, but to priorly flag them up, evaluate them and to finally value their risk for the organisation. The actual approach is seen in the identification of critical processes or areas which are worthy of protection and their corresponding resources (Swissbanking 2013).

In this context the term Enterprise Risk Management (ERM) is relevant to mention.

"ERM is a process, effected by an entity's Board of Directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."(Hiles 2011)

This definition covers various concepts and is therefore relatively diverse. First of all, enterprise risk management is an ongoing process through the entire organisation. Besides, it has effects for all hierarchy levels and individuals of an organisation, from the executive board to every individual employee in all divisions. ERM plays an essential part when it comes to the overall strategy setting of an organisation. The main task of ERM is to identify incidents or occurrences which will have impacts for entities, divisions or whole companies. Thereby ERM tries to reach its categorical targets, which may be also interrelated (Hiles 2011).

The following figure shows the huge number of different components that are all part of enterprise risk management.

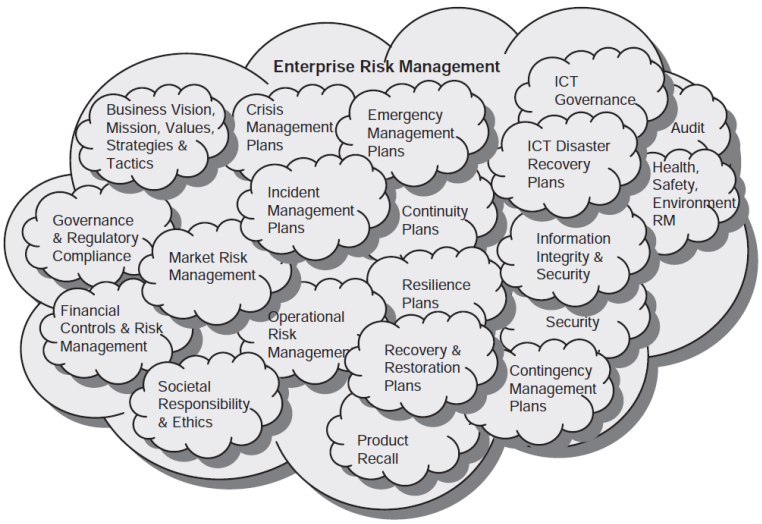


Figure 4: Governance, Risk and Plan Relationships (Hiles 2011:20)

In particular operational risk management has a major role within enterprise risk management because it could provide advantages for the whole organisation as the following subsection will show in more detail.

4.5.1. Operational Risk Management

According to the Basel Committee on Banking Supervision, operational risk is defined as the following:

"risk of loss resulting from inadequate or failed internal processes, people and systems or from external events"[6]

The definition´s fundamentals are based on the banking industry; however, the description fits to many other branches as well. A further definition states that operational risk is

"(...) in fact, it is a facet of every organization and reflects the inevitable fact that assets, processes and people can fail, leading to effects that are unplanned and unwanted by the business."
(Robinson In: Hiles 2011:66)

Operational risk is valuable for any organisation. The following example shows how operational risk management provides advantages for the whole enterprise. Due to rapid changes in a business´s environment, the threat that not all risks are captured at once occurs. Therefore, operational risk management strives to cover most of the risks in a systematic manner by paying enough attention to different kind of hazards in- as well as outside of the organisation (Robinson In: Hiles 2011).

4.5.2. Operational Risk Model

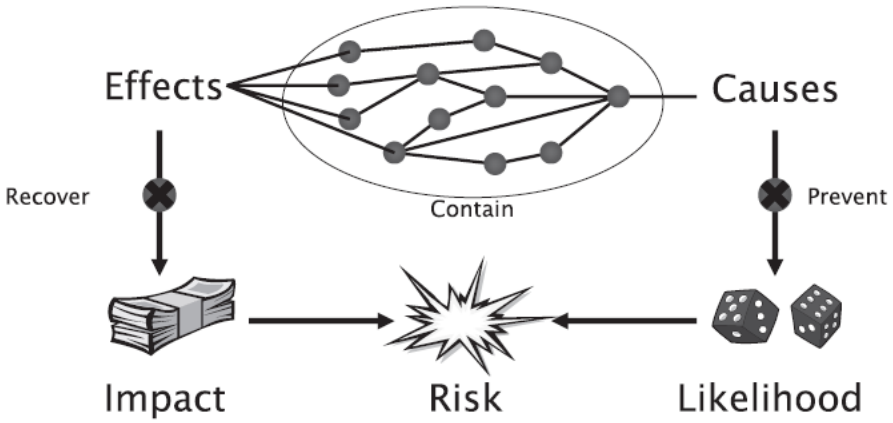


Figure 5: Operational Risk Model (Robinson In: Hiles 2011:70)

The Operational Risk Model (ORM) is a system that shows how operational risk could be managed. It relies on the comprehension of the elements – loss and probability.

While loss on the one side consists of many variables, like for instance lost regarding an organisation´s competitive situation, lost sales or losses regarding turnover, probability on the other side stands for a specific event to occur. This shows that many operational failures are mostly unforeseeable and a statistical classification is rather difficult to define. While loss is represented on the left side of the

[6] Basel Committee on Banking Supervision (2011): Principles for the Sound Management of Operational Risk. Bank for International Settlements. Basel, Switzerland. P.3

model, the likelihood of an incident to occur is shown on the opposite, the right side of the model. Natural disasters, terrorism or other threats and hazards are represented as Causes within the model.

According to (Robinson In: Hiles 2011), an enterprises risk profile consists of:

- *The Hazard Profile* which shows the significance of threats based on an organisation´s environment, area of activity, etc.
- *The Loss Profile* which demonstrates the effects of the losses that occur after an incident
- *The Gap Profile* which points out the defence readiness of an organisation in the sense of the identification of gaps

(Robinson In: Hiles 2011)

There is a continuous flow around the model, which may be interrupted by different kind of risk. Impacts which may disturb or change the flow are for instance the reduction of threats, the filling of gaps or the improvement regarding recovery measures. There is a reciprocal relationship between effects and causes based on their mutual influences (Robinson In: Hiles 2011).

Figure 5 shows, that the operational risk model is an adequate model that demonstrates why the issue of BCM is of that high relevance for organisations. The model represents many components that have an essential impact to BCM, like for example, the consequences of the so-called exposure of risk which is the sum of the expectations to gain losses from an unscheduled event with negative effects to occur (Robinson In: Hiles 2011).

For a smooth and efficient mode of operation, the ORM lifecycle prerequires other tools whose results flow into the ORM, like for instance the BCM-Lifecycle. Besides other components the results raised of the BCM-Lifecycle contribute to the proper functioning of the ORM. Therefore, the following pages will focus on the BCM-Lifecycle (Robinson In: Hiles 2011).

4.6. The BCM-Lifecycle

BCM in an organisation is based on the idea of a lifecycle. The lifecycle consists of four areas: comprehension of the company, the determination of an adequate BCM strategy, the development or implementation process and finally, the maintenances of the system, like for instance regularly updates that have to be conducted or general reviewing procedures.

Figure 6 illustrates the four categories (Cornish In: Hiles 2011).

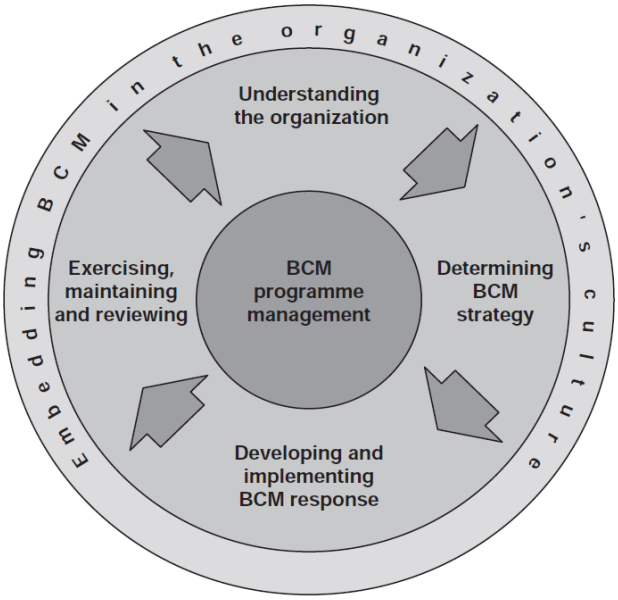


Figure 6: The BCM-Lifecycle (Cornish In: Hiles 2011:124)

4.6.1. Understanding the Organisation

This first step is seen as the basis for all further steps of BCM development in an organisation. It consists of the identification of an organisation´s objectives, activities or critical processes, assets as well as resources and stakeholder's interests and liabilities. For an optimal implementation of BCM all participants who stand in any relation to business continuity of a company X have to understand the issues listed. Additionally, people in any relation to BCM should promote the importance of it through the entire organisation. By identifying those bullet points more clarity is reached regarding priorities of an enterprise´s products and services.

Before the lifecycle moves to the second component which is the development of a BCM strategy, potential threats that may endanger critical activities and their corresponding resources have to be determined. Besides, the corresponding in- and external networks of a critical process or resource that may be affected in the situation of a crisis have to be identified as well (Cornish In: Hiles 2011).

4.6.2. Determining BCM-Strategy

The main purpose of this part of the BCM lifecycle is to determine a BCM-strategy that makes the recovery of critical resources and services possible within the set recovery time. Before the best-fit strategy is selected which is the one that shows the optimal appropriate response in the case of an incident, various strategies are evaluated and compared to each other. By selecting the appropriate strategy, aspects like resilience or countermeasures in the situation of crisis should be kept in mind (Cornish In: Hiles 2011).

4.6.3. Developing and Implementing BCM Response

BCM Response is that kind of action that takes place after an incident has occurred. This component of the lifecycle covers the BCM plans that are firstly examined and afterwards implemented to the organisation. These plans shall provide guidelines and are mainly preconfigured for the dealing with incidents by guaranteeing a quick process of restoration. Besides, a specific management framework is created and a plan regarding the management of crisis is evolved (Cornish In: Hiles 2011).

4.6.4. Exercising, Maintaining and Reviewing

The final component of the BCM-lifecycle is one of the most relevant concerning the long-term success of the system. In order to ensure the system´s effectiveness over a long period of time, it has to be ensured that critical assets and services are constantly evaluated on a regularly basis. The internal as well as the external environment are developing and changing fast. A possible countermeasure to take to encounter this issue are the performance of updates and upgrades.

This implies that critical parts or processes are identified and captured that may be critical at first but become less critical after a certain period of time, due to the changing environment. Naturally, this phenomenon also applies vice-versa. For this reason, periodic reviews are necessary (Cornish In: Hiles 2011).

The identification process at which stage an organisation finds itself at a certain moment within the BCM-lifecycle is not easy. There are several guideline questions that support the identification process. Those cover for instance questions concerning systems that are currently in use instead of BCM, emergency and recovery plans that presently exist or the organisation´s main doubts regarding BCM. Basically, the BCM-lifecycle has to be understood precisely on all levels of an organisation, as it is seen as a condition to build the future BCM vision.

The components that need to be considered concerning the development of an organisation´s vision are to set the future goals, to list the issues that shall be achieved or improved through BCM, the clarification of stakeholder´s needs and expectations, the planning of resources, the financial scope, the definition of the customers that should be targeted and finally the legal requirements that the organisation is operating in. By defining the organisation´s vision the advantages and benefits that BCM provides for the entire organisation have to be kept in mind as kind of an incentive to motivate all divisions of an organisation to participate.

After the vision is formulated, the last step of the BCM-lifecycle covers the composition of the strategy paper. The document shall list the objectives, the benefits, the personnel accountability during the process of implementation, the specific procedures of the implementation steps and indicators for the measurement of success of the BCM implementation process (Hibberd In: Hiles 2011).

The BCM-Lifecycle consists of various tools. One of those tools is the Business Impact Analysis (BIA) which is a tool that highlights all the critical processes and their corresponding processes of an organisations which are particularly worth protecting. The BIA is a common analysis that is conducted for instance at Deutsche Bahn for various company-specific applications.

4.7. Business Impact Analysis (BIA)

The Business Impact Analysis is a tool that is of high relevance for an organisation to identify its critical areas, like for instance processes and the resources that are necessary for the recovery process of a specific business segment. Furthermore, it shows the interdependencies between the individual processes. Besides, it shows the effects concerning business activity or the failure of a business-critical operation after an incident occurred (Swissbanking 2013).

Under the application of the Business Impact Analysis (BIA) all divisions within an organisation define their critical resources. Consequently, an extensive general overview on assets, services, operating processes which are especially worthy of protection can be generated by including all business units. The risky and threatened resources are allocated to the BCM system of an organisation afterwards. By

implementing all business areas to the analysis process critical dependencies between different departments come to light. This aspect is very relevant, as it shows the interconnectedness in case of an incident within a corporation. A kind of chain reaction can be determined in the sense of process dependencies.

In this context, the Recovery Time Objective (RTO) has to be particularly considered. The RTO is defined as the repair time a certain business-critical process needs for operating again. The RTO has already been illustrated in the beginning of the thesis in figure 2 and showed the significance of BCM with respect to the procedure of an incident. It has been found that the course of a crisis will lead to less fatal consequences for an organisation if a BCM-system is implemented (BSI Standard 2020, BC 200-4).

In the context of the RTO, the scope of components and resources that are relevant for reaching the pursued level of recovery are determined. In other words, which other resources or what kind of employees are needed for ensuring an efficient recovery point.

In order to be up-to-date, it is preconditioned that the BIA is reviewed on an annual basis.

4.7.1. Purposes of the BIA

According to Barnes (2011) data that is computed of the BIA is used for the following further purposes:

- Determination of processes, resources or entities and their relations to each other
- Identification of business-critical processes
- Basis for the further development of a BCM-strategy
- Evaluation of an organisation´s risk appetite (based on their financial investments that business continuity requires)

(Baumann & von Rössing In: Hunziker & Meissner 2017).

In order to achieve a successful recovery, the following components, which are also known as the Business Recovery Options (BRO) have to be determined: Staff, buildings, infrastructures, potential outsourcing partners and collaborations. The BRO are relevant for the proper functioning of an organisation.

After the BRO are set, the following step is the implementation of the previous defined components to the actual Business Recovery Plan (BRP).

Business Recovery Plans constitute the applied procedures and the utilized replacement resources which are highly required for further continuity of businesses as well as for the recovery of crucial processes. It is relevant that the BRP is always up-to-date. Therefore, the review of the plans should take place once a year. In the case of significant environmental changes that have impacts to whole business operations, the periodic review should be carried out more often (Swissbanking 2013).

The BCM-Lifecycle process covers first approaches concerning an understanding of the organisation to the final most relevant component regarding long-term success, the exercising, maintaining and reviewing of the critical assets and services of an organisation (Hiles 2011).

The BCM-Lifecycle should be further illustrated by means of a realistic example from practice. Therefore, the following paragraphs will provide an overview of the BCM-Lifecycle process of Deutsche Bahn.

4.8. BCM-Lifecyle at DB

The BCM-Lifecycle at DB is considered as a management system which should be used for the implementation and construction work of a BCM-system. It consists of the phases: analysis, strategy development, implementation and validation. In general, the provision of the BCM lifecycle is quite similar to the one presented in the theoretical BCM-part of the thesis (Cornish in: Hiles 2011).

The following table summarized the individual BCM-Lifecycle steps at DB.

BCM-Lifecycle I.:	**BCM-Lifecycle II.:**	**BCM-Lifecycle III.:**	**BCM-Lifecycle IV.:**
Pre-scoping, BIA, RIA	Strategy Development	Implementation-Process	Validation-Process

The single steps will be analysed in more detail within the following paragraphs.

4.8.1. BCM Lifecycle I.: Pre-scoping (Vorscoping), BIA, RIA

The first stage of the BCM-Lifecycle consists of Pre-scoping (Vorscoping), Business Impact Analysis (BIA) and the Risk Assessment Analysis (RIA).
Pre-scoping is understood as the damage evaluation for the preselection of the subsequent BIA that is conducted. Damage of each business process is evaluated separately according to its operative, financial, regulatory aspects, as well as its reputation. In this context, certain critical business processes are identified for the first time. Afterwards the actual conduction of the damage evaluation follows. While the results are on the one side the business-critical business processes that come to light, on the other side the procedural dependences including their required resources become visible.

In the following step the identified critical processes have to be evaluated concerning the consequences their failure would mean for DB. This step is carried out with the help of a risk assessment analysis (RIA). A risk matrix that covers the probability of risk to occur is a tool that is applied by the BCM-Division in this context. It constitutes the identification and elaboration of potential hazards, including an analysis of the probability of occurrence as well as the extent of damage which lead to the malfunctioning of critical processes. The BCM division at DB is mostly dealing with threats that are between *rare* (occurrence 1 to 5 times per year) and *expectable* (occurrence is more frequent than 1 time each 5 years). This implies the BCM division does not deal with hazards that occur several times a month. That lies more in the area of responsibility of the emergency management team of the division crisis- disaster- and emergency management.

Risks are calculated by the usage of tools, like for instance risk security invest calculations, benefit analyses and risk matrix visualisations. The performance of risk assessments is essential because decisions are always made on the basis of risk. In addition, also BC-plans and the implementation of measures are always prepared and carried out in conjunction with the DB risk classes. There are strict guidelines, from which risk class onwards a certain BC-plan has to be drawn up or an IT emergency plan has to be created.

To sum up, the BCM-division at DB is rather dealing with major issues that could lead to serious consequences for the entire organisation, like for instance terrorism, cyber-attacks or blackouts.

In summary, the Pre-scoping-process rests upon an initial damage assessment to certain business-critical-processes on the basis of specific criteria. These first steps are a kind of pre-prioritisation in order to sort out processes that are not urgent to DB. The general purpose is that after the pre-prioritisation phase took place, only those processes are implemented to the system, that are associated with potential risks. In order to attain an objective evaluation, the risk evaluation is based on predefined factors, like operative, financial, regulatory, reputation and danger to life. Finally, a list of potentially critical business processes is gathered which are subsequently again addressed in the BIA.

At DB, a business impact analysis is understood as a damage assessment. The focus is not on how likely it is that a certain process will fail or the reason for failure, the focal point lies more on the consequences of the process malfunctioning. This implies that the interests are seen in the question what kind of damage would the failure generate for DB. Therefore, the components Pre-scoping, BIA and RIA are considered as significant parts of the whole BCM process. For adding a certain risk to a critical process, the process has to be identified at first (BIA). Afterwards the steps of the determination of the maximum tolerable downtimes for the respective critical business processes, transparency regarding the dependencies between the business processes, the identification of the required resources for the critical business processes and the determination of the level of performance regarding the resources in times of daily operation as well as for the emergency operation and thus also the restart parameters could be carried out.

The results of the BIA and RIA are compared on the basis of standardized damage categories which are represented as a table that consists of different damage categories and damage levels. It is cut down in an operative-, a financial-, a regulatory-, a reputational- as well as danger-to-life aspect. (It should be mentioned that the category danger to life consists just of two components –danger to life and no danger to life.) Subsequently, each of these components has different risk levels between the numbers 1 to 4. Category 1 represents low damage, while 4 illustrates the highest level of risk or damage. The following example sought to contribute to a better understanding of the table.

Example: Regulatory

The damage category of regulatory covers inter alia the aspects of GDPR (General Data Protection Regulation) or KRITIS-standards which are based on the guidelines provided by BSI. Under damage level 1, which represents the lowest level of potential danger, the regulatory includes an individual case which covers political or legal aspects. Under damage level 2, the risk or threat increases slightly and an individual matter will definitely lead to a legal or political review with already foreseeable consequences. Level 3 of damage refers to a situation or series of situations that bring legal or political consequences for parts of the company as a consequence. The highest level of danger is seen in damage level 4. Level 4 means an issue or a series of issues that lead to critical legal or political outcomes for the entire company.

Example: Reputation:

Within the category reputation, the focus lies on the image of DB based on the media reporting. Based on the company size and the importance of DB throughout Germany, the organisation is obviously quite often one of the main issues in press releases. The purpose of "reputation" is to identify how critical the reporting, articles etc. are about DB Group. Critical in this context means, how DB image might sustainably be endangered.

The Application of a Risk Matrix

Furthermore, DB applies a so-called risk matrix to their BCM lifecycle model. In more detail, the BCM team of DB evaluated a risk matrix that is based on a number of risks and their dependence between their probability of occurrence and extent of damage. The matrix is actually the result of the risk-identification, the following -analysis and evaluation of it. The aim of the matrix is to clearly highlight the risks that represent the most urgent to deal with. The aim is to link critical business processes with threats and their probabilities to occur.

The actual value is based on the product of the extent of damage, which is the result of the level of damage taken out of the pre-conducted BIA and the probability of occurrence. The values lie between 1 and 16. The higher the calculated value, the higher the level of risk for a following potential damage. Furthermore, the values are divided in A (value 1), B (value 2-3), C (value 4-11) and D (from value 12). While value 1(A) requires no obligatory actions to be taken by DB, the values B, C and D definitely require some kind of action or measure.
While at value B risk acceptance is still an option, at value C and D risk treatment is indispensable. If the risk lies within the value range (from 12 upwards), ad hoc measures have to be taken fast, in order to counteract the threat, at least until technical risk measures have been implemented. These steps are accompanied by certain reporting obligations.
With the help of the assignment of various numerical values, one would like to define a kind of critical quality that is no longer acceptable and tolerable, as the consequences for the DB Group would be really serious. Basically, this step is conducted for the creation of a comprehensive overview that highlights which processes stand in relation to the critical ones. Furthermore, one wants to identify which other infrastructures, personnel, resources or plants are affected and how recovery parameters look like, in the case a process gets interrupted.

In order to obtain meaningful and correct results, the individual partial steps of the analysis phase must be analysed and reviewed regularly.

Based on factors like for instance new technologies, digitalisation, newly emerging crisis, influencing variables are changing. While one year the focus of the risk identification process lies within a certain field, this risk area may be out of scope and completely irrelevant for an organisation a few years later. Therefore, risks in general have to be constantly newly evaluated.

In this context, the individual risk classes of DB Group are developed jointly by the BCM department and the respective professional disciplines. Operational Risk Management, that illustrates how operational risk, like for instance the loss that occurs due to the failure of processes could be managed, visualised the risks which are relevant for DB. This could be for instance conducted by the application of risk matrix.

In general, the risks are reviewed once a year. If special events occur, for example in the event of a certain crises or general restructuring measures, the risks are evaluated more often.

4.8.2. BCM Lifecycle II.: Process of Strategy Development

BCM Lifecycle II covers the development of initial strategy-approaches. Based on the results of the analysis, risk treatment options are developed and selected. The risks of all relevant business processes from the RIA are summarised in a so-called "risk inventory". Subsequently, the results of the strategy phase emerge that consist of the determination of the risk owners, the presentation of possible risk treatment options and the assessed remaining risks.
The BCM strategy at DB is developed in line with the group strategy. The BCM strategy is always derived accordingly from the new corporate strategy so that there is no contradiction between these two.

4.8.3. BCM Lifecycle III.: Implementation-Process

Within the implementation-process the main focus lies on the establishment of business continuity plans (BCP). Thus, based on the analysis and strategy phase, risk-preventing measures are implemented in this phase and concrete business continuity plans are firstly drawn up.
The aim at this stage is to put the gained knowledge into practice and to check the effectiveness of the risk-related measures, which have been developed previously. It is important to mention that a documented measure in theory does not necessarily work in practice. Therefore, the effectiveness of the measures developed still has to be verified. If the verification process is completed successfully, the BC-plan can finally be established.

The BC-plan includes all relevant information regarding a specific critical process. From initial thoughts and first considerations to concrete parameters, like for instance the risk-combination within the framework of a plan, the corresponding starting times of certain resources, further processes of the related network that are affected in the event of a disruption, etc. –the BC-plan has to contain all the relevant information.

Special attention at this stage has to be paid to particularly critical disruptions and incidents - for example, a widespread power blackout or a pandemic. For these scenarios, separate BC-plans should be developed which guideline how to proceed in these kinds of scenarios. Concrete measures regarding further courses of action are recorded within the plans.

The implementation phase constitutes besides the conducted business impact analysis one of the main activities of the BCM division at DB Group.

4.8.4. BCM Lifecycle IV.: Process of Validation

In the final phase, the validation phase, the functionality, effectiveness and appropriateness of BCM is assessed through regular exercises and reviews. If necessary, corrective measures are taken.
In order to be well-prepared for all kind of incidents, the process owners of the respective processes are always involved in emergency exercises and test runs.
The results of the validation phase are finally evaluated and flow back into the next BCM lifecycle. In the end, also audits play an important role regarding the review quality. Overall, each individual phase of the BCM lifecycle has to be regularly reviewed and if necessary, adaptations have to be made. This guarantees that an organisation is always up-to-date regarding their business-critical processes, all relevant and critical processes inside an organisation are recorded, each modification of a certain process is captured and that they fit the altered parameters. The general achievements of operations by the BCM-division at DB are measured by key performance indicators and the degree of maturity, like for instance the number of processes for those specifically BC-plans already exist. In this context business continuity testing is significant.

4.9. Business Continuity Testing

Business Continuity Tests are verification procedures which are conducted for testing the efficiency of the own systems. One of the results is that it will become clear, how effective disaster recovery plans are and how efficient an organisation´s capability to manage a crisis is. An interesting aspect in this sense is the outcome by testing different divisions parallel. The simultaneous testing leads to an entire view how the organisation is dealing with the issue crisis (Swissbanking 2013).

In conclusion of the BIA-subsection, it can be said that, the main aim of the BCM-Lifecyle is to illustrate single BCM-steps and to put them into a consistent framework in which the individual components build upon and are dependent on each other. In this context, ISO standards represent a possibility for a structured implementation of the BCM-Lifecycle. ISO stands for Security and Resilience Business Continuity Management Systems – Requirements which is the first developed standard on an international basis, that could be applied to any organisation. The guidelines include all steps that are required for the implementation of a BCM system and generally aims to reduce risks within companies (BSI Standard 2020, BC 200-4).

The results of the insights gained by conducting the certain steps of the BCM-Lifecycle can be used for the construction of Business Continuity (BC) Plans which will be further analysed under the following section.

4.10. Business Continuity Planning (BCP)

Business Continuity Planning consists of Business-Continuity-plans that are pre-developed scenario or process-dependent that address a tactical approach to the occurrence of a specific crisis. For example, the Red Cross has a BC plan that has been developed in cooperation with the City of Vienna for the scenario of a blackout. BC-plans cover event-specific guidelines to follow and measures to take for dealing with a specific event.

The German BSI (Federal Office for Information Security) gives a further precise definition of BCP.

> *"Strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level."*
>
> (BSI Standard 2020, BC 200-4)

The origin of business continuity comes from the field of disaster recovery and is nowadays strongly ingrained in the field of IT. The following paragraph highlights how BCP supports the organisations regarding the strategic decision-making process (Ramakrishnan & Viswanathan In: Hiles 2011).

Risks in general developed and changed over time. While in the 1970ies risk were less abstract than today, the main problems that had to be faced, arose due to machinery or plant issues and labour. Based on the progressive digitalisation, risk got more intangible, broader and generally complex. Knowledge for instance represents a key factor when it comes to the more intangible threats (Ramakrishnan & Viswanathan In: Hiles 2011).

Speight (2011) identified four levels of business continuity planning: Mitigation, Readiness, Response and Recovery. Mitigation is related to the diminishing process of threats and the general dealing and handling of risks within the organisation. Readiness refers to the company´s preparedness regarding the risk management´s pre-developed measures and plans of actions in the case of an incident. Response is the actual handling of the emergency after it occurred and the term recovery refers to the identification process concerning the needs for returning to the normal state of business operations (Speight 2011).

To sum up, BCP follows a strategic and tactic management approach and strives to support the decision-making process of an organisation during an incident. Therefore, BCP represents an important component concerning the long-term strategic orientation of an organisation. For this reason, the following paragraph will take a closer look at the strategic aspect of BCM and will illustrate how the development process of a BCM-strategy could look like.

4.11. The Development of a Business Continuity Management Strategy

When it comes to the process of the effective development of a BCM strategy, one of the main challenges is to ensure that the BCM strategy is developed in line with the organisation´s business strategy. There are various aspects that demand attention, during the development process. One should initially find out the scope of BCM for the organisation. The scope shall therefore be identified and determined. Besides, the BCM strategy shall be embedded within the organisation. Furthermore, a governance structure has

to be developed and aligned to the original organisation. The step that follows, covers the definition and the allocation of responsibilities. This step must be taken into account seriously, as the selected persons have the major impact to manage and lead to common achievements and success of the business continuity management within a corporation. In addition, potential threats shall be monitored in relation to their impacts on organisation´s resources. Moreover, the frequency of occurrence in which tests and plans will be carried out has to be determined. Finally, the reporting system as well as the reporting period and further developments have to be defined (Swissbanking 2013).

An appropriate development of a BCM strategy is crucial for an efficient implementation process. For the development process the definition of vision and mission is crucial. The mission and vision are considered to relevant for the target/actual comparison of key performance indicators. Therefore, it is necessary they are priorly defined. If the mission has not been defined, financial indicator, like for example ROI (Return on Investment) or EBITDA (Earnings before interest, taxes, depreciation and amortization) are mainly used to provide information about an organisation´s performance concerning the process of strategy development. However, if there is a mission statement there are several approaches that could be applied for the strategic planning process. One of those is the so-called Balanced Scorecard Approach which will be analysed in more detail under the following subsection.

4.11.1. The Balanced Scorecard Approach

The balanced scorecard approach represents a tool often used by the strategic planning of an organisation Basically, strategy follows a long-term approach; therefore, the development process requires a long planning horizon, in which the definition of a company´s mission should have already taken place.

When it comes to the implementation of BCM, it is important to go in line with the business strategy. The following paragraph analyses four perspectives that are necessary to consider, when it comes to the application of the balanced scorecard approach (Hibberd In: Hiles 2011).

The four components which were developed by Robert Kaplan and David Norton shall provide managers a kind of measurement framework to analyse an organisations performance.

The aim is to combine an organisation´s non-financial as well as financial performance measures for harmonising the holistic approach of a company´s efficiency. The critical success factors (CSFs) which are established from the vision and mission statements, consist of the following components: Financial, Customer, Internal and growth (inclusive further development) are defined. Key Performance Indicators (KPIs) are formed on the foundation of the CSFs. By establishing destinations or targets and by implementing specific plans (actions) of procedures or projects to each of the four components, the KPIs shall be fulfilled. All of the procedures presented above shall be conducted in line with the business strategy of an organisation for guaranteeing that the BCM strategy is as well targeting an organisations mission achievement and pursuing the same vision.

Figure 7 provides a brief overview of the components presented above (Hibberd In: Hiles 2011).

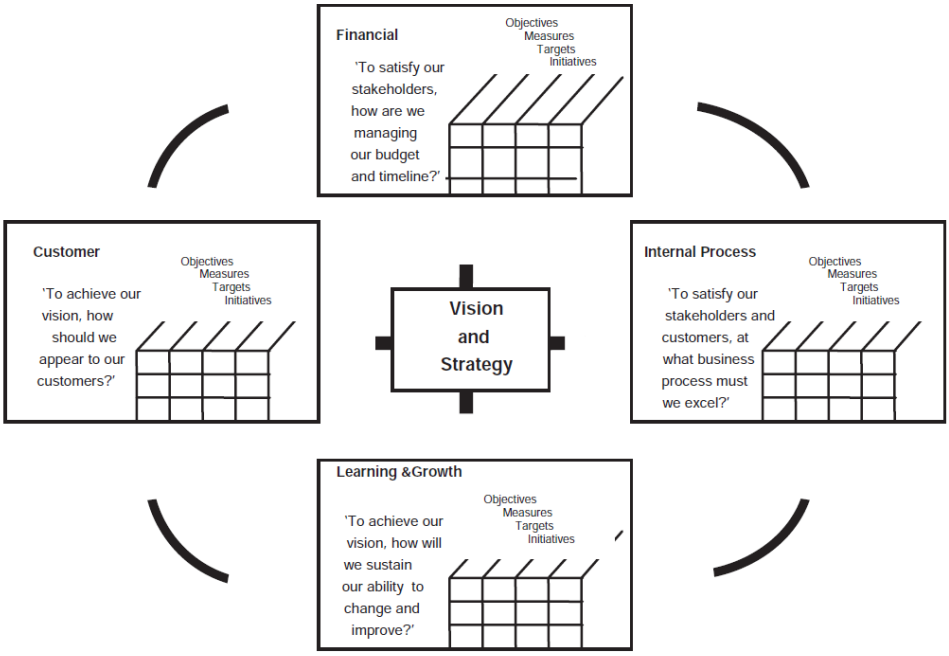


Figure 7: The Balanced Scorecard Approach (Hibberd in Hiles 2011:26)

The challenging part in this sense, is that the threat of ignoring an organisations business strategy by "incorrectly" conducting the balanced scorecard will lead to the outcome that the followed vision of the BCM strategy is not in line with the actual business purpose. Additionally, this leads to miscommunications with the stakeholders of an organisation and the incorrect applications in times of crisis, which may cause fatal consequences (Hibberd In: Hiles 2011).

To sum up the Balanced Scorecard Approach is an appropriate method to develop a BCM-strategy that goes in line with the organisation´s strategy. The main aim is to develop a strategy that is supported by the entire organisation and that shows flexible and innovative features as it could be easily adapted in the case that the company´s strategy changes. The implementation of the management is highly relevant as this implies that awareness for the issue of BCM through the organisation increases. As a result, support of become visible which further leads to a proper implementation process of the BCM-strategy into the organisation (Hibberd In: Hiles 2011).

The BCM-strategy is necessary to be set for the actual deployment of the Business Continuity Management System which takes place afterwards. The approach will be presented below.

4.12. Business Continuity Management System (BCMS)

A Business Continuity Management System (BCMS) is a variety of tools and instruments that are applied by a company for designing its strategy and putting it into practice. Additionally, it includes the reviewing tasks, like for instance the monitoring of the BCMS which takes place after the strategy has been established and the regular inspection of the system´s effectiveness (Wong 2014).

When applying a management system to an organisation it is relevant to follow guidelines, like for instance those specified by the management (e.g., company-specific objectives). Within the application process someone can distinguish between three levels (1 – 3). Level 1 has as its objective the awareness creation concerning a certain object. To achieve this goal, internal audits have to be conducted. This is

mainly for management reviews. Level 2 is related to the development of compliance standards within the organisation which consist of the implementation of a management framework in the business processes. Finally, Level 3 of application which covers the certification. This step concludes the previous levels by certifying the management system and the establishment of a policy guideline to the business operations (Wong 2014).

Now, that the strategy approach has been defined and the activities concerning the Business Continuity Management System have been conducted, the question after an appropriate embedding process arises. For this reason, the following paragraphs will deal with the issue of embedding BCM to the organisation.

4.13. Embedding BCM

The BCM embedding process covers four areas which are summarized in figure 8. The initial step is the initiation, followed by the planning for business continuity, the stage where the actual strategy implementation takes place and finally the operational management.

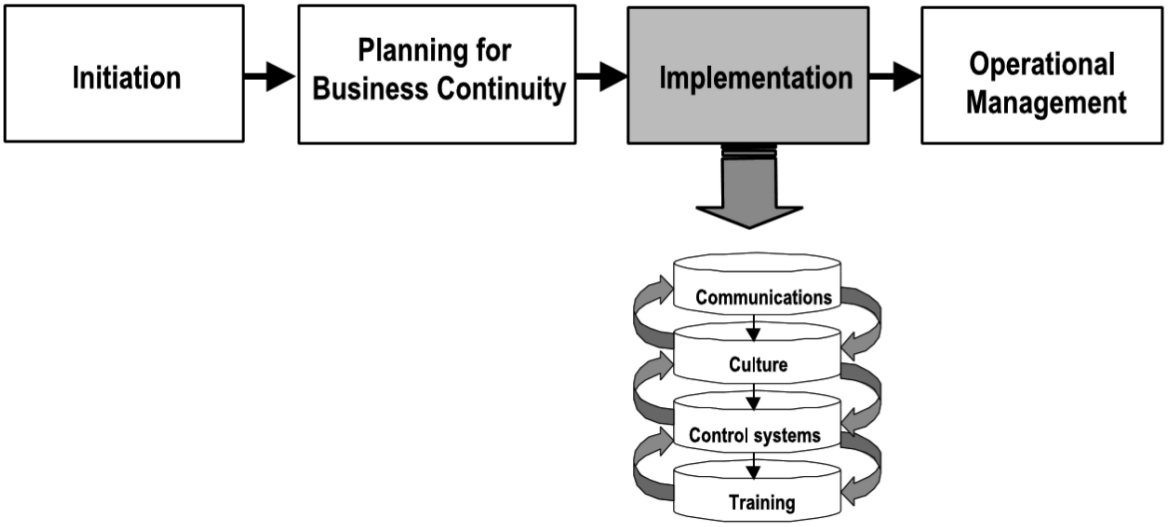


Figure 8: Embedding BCM (Swartz et al. 2010)

First of all, it is relevant to keep in mind that the successful embedding process of the previously finished BCM-strategy and the corresponding BC-plans requires the following two conditions: clear organisational structure and organisational conditions.

The first one is related to the structure of an organisation. This prerequisite that the company shows explicit structures, spheres of responsibility and allocation of tasks. In this context, the available management undertakes a lead because of their driver-role regarding the entire BCM-process. The management has to ensure that the implementation process is holistically conducted. Key tasks of the management at this stage are for instance monitoring tasks and issuing instructions The second prerequisite concerning the proper implementation process is the accurate preparation of organisational conditions which cover for example a proper flow of communication and control mechanism (Swartz et al. 2010).

As already mentioned, it is important to consider during the entire implementation process that BCM is part of the whole organisation. This issue clearly arose during the expert interview with Red Cross, where BCM is even understood as part of the aid organisation´s DNA. It is therefore essential to keep in mind that the implementation process will always be conducted company-wide. In the case, that the homogeneous implementation process is insufficiently followed, the whole realisation will not lead to great success. This is for instance the case, if a single individual takes responsibility for the embedding process, instead of the entire management team. In this kind of scenario subjective assumptions or beliefs about for instance the organisation´s vision led to misunderstandings and failures which affect the entire implementation phase.

There is no consistent approach to be followed regarding the implementation itself. It is more up to the organisation itself how the first step will be tackled. In this sense, there are various options, like for instance the usage of material that is already available, like for instance the developed mission and vision statements. At this stage, the aim is to deepen the knowledge about the organisation. A potential option in this connection is to conduct interviews with single employees or groups that serve in a specific business. Questions about economic parameters, organisations objectives, target groups, factors for success etc. are raised in this context and will lead to more insights that as a result will guide the organisation through the initial implementation steps. Additionally relevant to consider, is the stage at which the organisation finds itself at the BCM-Lifecycle when the implementation takes place (Hibberd In: Hiles 2011).

Implementation always stands for change. Change is often connected to uncertainty and internal- as well as external pressures that will put new challenges to an organisation. Pressure, in turn, may consist of company-related issues or generic stimuli of a certain field of activity. (Swartz et al. 2010) In this context, Lewin (1951) argued, that all kind of change in an organisation demand for the so-called “unfreezing” of a situation which stands for an openness to modify the status quo. Afterwards the planned transformation is issued and finally, the new state of affairs is “refrozen” again. Lewin´s force-field analysis precisely aims at these different stages of change. While the conclusion in the beginning implies that there is demand for change, the following steps cover the finding of the new optimum state of affairs, the unfreezing process, the realisation of the change and finally, the refreezing process (Lewin 1951 cited from: Swartz et al. 2010).

BSI (200-4) names the concrete steps of the implementation process of a BCM system to a company. After the decision of the BCM-implementation has been taken, the primary responsibility is assumed by the top management of an organisation. Subsequently a BCM agent is elected. The BCM representative is the main contact person regarding all belongings in connection to BCM. The person coordinates BCM relevant tasks and acts a bit as a driver for the implementation process through the entire business (BSI Standard 2020, BC 200-4).

After the responsibility has been taken by the board management and the BCM representative has been elected, the initial steps of the development of the BCMS begin. The conception of the management system is built upon six steps, that could be seen as kind of guidelines for a proper BCMS-realization.

4.13.1. Step 1: Definition and Distinction

In the first step the definition and distinction to other already established management systems is conducted. The aim is the identification of processes that cover parts of BCM and constitutes an interface. The first step is mainly to prevent systems from duplicating work and blocking each other in some sense.

4.13.2. Step 2: Definition of the BCM-Organisation

All responsibilities of BCM are captured in the so-called BCM-organisational structure. It covers the emergency prevention organisation as well as the emergency management organisation. The first consists of all the positions that are responsible for BCM –either regarding the development or the maintenance services. The emergency management function is to handle the challenges after an incident occurred. It comprises all kind of tasks that are needed for the recovery of an organisation. It is also called the `Besondere Aufbauorganisation (BAO)´ which stands for the `special organisational structure´. In this sense BSI (200-4) lists three different acting-levels of the BAO. Those comprise the strategical, the tactical and the operational level of BCM. While the strategic component covers all of the goals and targets, it also sets the scope of application. This scope is taken up to the next level, the tactical stage where clarifications concerning the target achievement are made. Finally, the operative level is responsible for the development of concrete measures for accomplishing the defined goals (BSI Standard 2020, BC 200-4).

4.13.3. Step 3: Documentation

There are two types of documentation: the preventive and the reactive documentation. The preventive documentation defines the targets and identifies the general requirements for the business continuity management system (BCMS) from a strategic point of view. It thus provides the binding framework for all further activities and documentation processes of the BCMS. In more detail, it defines and records under what kind of conditions the BCMS is set up and operated, as well as the general objectives for the BCM. More detailed information for the BCM system is documented in the emergency preparedness concept. These documents define how the objectives of the guideline could be reached. The reactive documentation consists of an emergency manual that contains all information on emergency management. The contents of the manual vary from organisation to organisation due to variables like for instance the size or complexity of a business. During an incident, it is important that the manual is always available to the respective target group.

4.13.4. Step 4: Resource Management

It lies in the responsibility of the institution's management to provide the BCMS to adequate personnel, time and financial resources. The resource management depends on various factors, like for instance the size and complexity of the organisation, the internal structures, temporal targets, etc. Especially the costs concerning the financial resources can only be estimated in an early phase due to the fact that the precise costs become evident in a later stage of the BCM-implementation process.

4.13.5. Step 5: Trainings

A key success factor concerning the efficient establishment of a BCM system is the continuous development of skill sets and the knowledge of personnel that stands in any relation to the businesses' BCM system. Besides, training objectives are defined and the organisation has to check whether these have been achieved.

4.13.6. Step 6: Sensitization

For the long-term success of a BCMS it is crucial that besides the BCM role holders, all employees understand the importance of BCM. Therefore, awareness has to be raised and it should be ensured that almost all employees implement and maintain a desired behaviour of their own accord and conviction (BSI Standard 2020, BC 200-4).

To briefly summarise the previous paragraphs, the embedding process of the BCM-strategy is very time-consuming and is shortly described understood as the implementation phase where the main objective is to get the BCM-system practically run. To reach this goal, the conception of the six steps that need to be followed for ensuring a final BCMS-realization that is characterised by long-term success, is necessary to conduct.

However, there are many guidelines and catalogues that provide instructions how the implementation process specifically could look like, there are many malfunctioning Business Continuity Management Systems. There are various reasons for that which are briefly demonstrated under the next section.

4.14. Reasons for Malfunctioning BCM(S)

There are various reasons why BCM is relatively low established and particularly not well-advanced or not implemented at all in most organisations. Peterson (2009) stated that financial support plays an essential role regarding an effective BCM system. This issue is based on the missing ROI-aspect (return on investment) which is considered by many top managements. At the first sight, there is no financial benefit for the organisation during the first part of the implementation process. In most cases, the actual benefit or advantage of the pre-implementation of BCM to the organisation comes to light after a negative event occurred. Therefore, the comprehension of the benefits of a BCM implementation and its impacts on a businesses' performance is considered as one of the keys for the long-term success (Bakar et al. 2015b).

There are various reasons why, even after a successful implementation many BCM systems are not functioning as expected and which furthermore, won´t lead the organisation through an incident or crisis with the desired continuity. One of the main causes, is that the business continuity plan has not been carried out practically by the organisation. This implies that the implementation of BCM has certainly been conducted, however the step of the training process (for instance employee trainings) has not been conducted. This could lead to fatal consequences during an incident which are remarked in the lack of communication and as a result in information between different divisions.

A study conducted by Gingl & Buser (2013) highlights the fact of missing responsibilities. 40% of medium-sized companies that participate in the study argued that the responsibility of BCM rests at the CEO or the management board of an organisation. Solely every tenth organisation has a so-called business continuity manager. Businesses without a specific BCMS take the following measures to handle with uncertainties: Data backups and the conclusion of insurance contracts in the case of unserviceability.

To sum up most organisations are insufficiently prepared for the state of crisis (Gingl und Buser 2013). As a result, this insufficient preparation leads to a malfunctioning BCMS-system. However, there are possibility to address this issue. One of the main aspects in this sense is to put a specific focus on the critical success factors during the implementation phase.

4.15. Critical Success Factors during the Implementation Phase

It is relevant to take into account the critical success factors during the implementation phase for ensuring a proper functioning BCMS.

Critical success factors concerning the implementation phase of a BCMS have been identified by (Bakar et al. 2015b). They highlighted single components which should specifically receive attention: management support, external requirements, organization preparedness and embeddedness of continuity practices. The support by senior management is very relevant for BCM´s future success. The result of too less involvement of top management will lead to program failures. Besides, external requirements, like for instance governmental regulatory requirements have to be met. That implies that specific kinds of external formalities have to be complied by the organisation itself. In other words: the organisation has an external obligation (mostly issued by governments or customers) to guarantee business continuity. Regarding an organisation´s corporate governance those are the drivers for a greater

significance to the issue of BCM. The third critical success factor is an organisation´s preparedness. This means that the resilience of an organisation is strongly reliant on the company´s capability to prevent or to speedy recover from a potential incident. In this context (Herbane et al. 2004) defined that an organisation that has the ability to quickly recognize new threats and swiftly reacts to incidents, is said to have an advantage regarding organizational alertness. An organisation´s preparedness stands as well in a close relation to an organisation´s familiarity concerning different approaches of recovery and the general risk awareness. Finally, the embeddedness of the continuity practices follows. If the organisation is effectively and well-prepared in case of an incident, the operational business continuity processes are embedded in already established processes. The entire organisation will evolve into a stronger and more resilient business, based on the embeddedness into existing processes. As a result, the capability of the risk can be reduced to a minimum level (Bakar et al. 2015b).

The implementation phase is often underestimated by many organisations. Therefore, error-prone and inefficient BCMS are oftentimes the result of a too tight timescale concerning the implementation process. As Gingl & Buser (2013) argued the launch or introductory phase of a BCMS sometimes may even last two or three years in medium-sized enterprises. Therefore, the time aspect plays an important role for the proper functioning of BCMS. The time component forms together with the economic operation (like for instance a regular maintenance and the execution of updates) the actual basis of a successful BCM system (Gingl & Buser 2013).

Besides the critical success factors during the implementation phase there are further variables that could influence the effectiveness of a BCMS. Those influencing variables are strongly depending on the environment of an organisation that is mostly characterized by uncertainty (Hiles 2011).

4.16. Influencing Variables

The micro- and macro environment of an organisation covers a multitude of contingencies, which constitute a kind of threat to an organisation. The only way to deal with these potential risks is dependent on the organisation’s involvement of BCM by the management. The following paragraph gives a summary of various threats of an organisation in the form of influencing variables for BCM systems, that are all characterized by uncertainty (Bakar et al. 2015b).

There are thousands of influencing factors e.g., the environment, digitalisation, cyberattacks, financial markets, a scarcity of resources or supplies in general, information gaps, regulations and laws, terrorism and further that may impede a BCM system. Especially, the digital transformation process brought major changes to organisation´s BCMS because those systems had to leave the analogue world behind and develop to a digitized one. Many challenges arose in this context, like for instance the issue of dealing with high volumes and high-speed of data. As a result, systems got overload with information, like it is for instance the case at DB. Moreover, BCMS got slow and worked imperfectly.

The main threat of a bad BCM system is that it allows potential risks easier to stop or even destroy business processes. This results in losses, which have huge negative impacts for whole corporations. Therefore, the main goal is that a well-functioning BCM system will hinder the incidents to last long. A report published by Gartner Group in 2004, shows that USD 42,000 are lost per hour due to malfunctioning or even not existing BCM systems. (Bakar et al. 2015b) These costs represent expenses for service downtime. Ten years later, the outcomes of a survey, conducted by the consulting company KPMG highlighted that within the period of one year 36 % of the businesses analysed within the survey lose more than USD 100,000 due to the cost of downtime. Additionally, 12% of the companies examined actually write costs of downtime in the amount of more than USD 1 million (KMPG 2014 cited from: Bakar et al. 2015b).

Downtimes bring negative impacts and huge consequences for a company, not only in the form of capital. Besides, also a business's reputation, customer loyalty, marketing, an organisation´s effectiveness and efficiency, the quality, etc. are affected. However, it is important to handle this issue in all types and sizes of businesses (Bakar et al. 2015b).

Based on the digital transformation process, there have been major changes regarding the safety hazards of an organisation. It became clear that institutions in general became more and more dependent on information technology (IT). Besides, new risk emerged, like for instance cyber-attacks or extreme natural events due to climate change which could lead to a significant danger for whole societies. Among other things cyber-attacks aim to interrupt critical business processes which as a result lead to disastrous consequences for companies affected as well as their related stakeholders (BSI Standard 2020, BC 200-4).

However, new risks bring further challenges for the BCMS that organisation have to tackle, there are approaches to deal with new risk. The Multilateral Continuity Planning Approach is (MCP) is one of them and will be briefly present in the following section.

4.17. The Multilateral Continuity Planning Approach (MCP)

The Multilateral Continuity Planning Approach is one possibility to manage "new" influencing variables. While other approaches only put the focus on single components of impending risks, the approach of MCP is well-defined and basically, extends the planning measures. Business continuity is not a phenomenon that is just dealt within an organisation. It covers much more. In addition, the macroeconomic environment is essential. Contracting parties, suppliers, customers, partners, etc. shall all be considered in the process of continuity planning (Hamilton In: Hiles 2011).

For the efficient construction of multilateral continuity planning the conduction of awareness presentation is indispensable. By presenting the objectives and necessities concerning the relevance of MCP, awareness should be raised, especially the one of customers, suppliers and other key partners. Additionally, an appropriate level of comprehension and transparency shall be reached. The next steps include the establishment of a certain MCP project team and the establishment of a think tank. The main activities by the task force are related to the project coordination. The fact that MCP is relatively new for many businesses, shows up the opportunity to develop and creatively search for ideas by the creation of a think-tank. The so-called thinking factory should consist of senior representatives from different divisions. Various disaster scenarios and number of crises shall be discussed in the think tank (Hamilton In: Hiles 2011).

To sum up the MCP is an innovative opportunity for an organisation to deal with newly influencing variables by covering the internal as well as the external factors that have impact to a company´s BCM-system. By addressing these kinds of influencing factors, the BCM-system will improve as it can prepare measures for the handling of various scenarios in advance.

To briefly summarize what the thesis highlights in the previous paragraphs so far is the following: the implementation of a BCM has to go in line with the organisation´s strategy (in accordance with the vision and mission statements). After the implementation process has been carried out updates and regular maintenance should be conducted for ensuring that even newly emerging risks are captured early enough. Finally, BCM should follow a holistic approach which implies that the management team indeed has a key role regarding BCM responsibilities, especially in the context of awareness-building, however the entire organisation has to be involved in the BCM development process too (Gingl & Buser 2013).

Assuming that the implementation process has be conducted efficiently and the steps described in the previous paragraph have been implemented well, the question arises how the actual objectives of BCM look like.

4.18. Goals of BCM

The main objective of BCM is to prevent a complete collapse of a system in the case of an incident and to ensure that critical processes are still operable or quickly operating again. The aspect of a temporary interruption is therefore very relevant. While the key focus is often to secure organisation´s assets, like machineries, many times the protection of cash-flow processes gets lost. Within many companies the safeguarding of business processes, like infrastructures, information technologies or in-house communication processes represent subsections which often get too little attention concerning security measures for business continuity (Gingl & Buser 2013).

Besides, the focus of BCM is to ensure critical processes to continue at the moment of an incident. A minimization concerning the financial and legal impacts as well as an organisation´s image will be pursued. In conclusion the objective is seen in the field of rapid business or business processes recovery one the one side, and the general business continuation on the other side. In other words: an organisation implements BCM for improving their capabilities to deal with any kind of incident or crisis (Swissbanking 2013).

In the achievement of the goals, the BCM plan plays a relevant role.

4.19. The Value of a BCM-Plan

The value of a successfully evolved BCM-plan is therefore very important for an organisation. This is due to various issues. Firstly, it is based on the organisation´s ability to point out the risks it is confronted with and the lead of management responses. Secondly, it rests on the capability to safeguard corporate´s interest and business processes. Thirdly, the BCM-plan highlights how an organisation is prepared concerning the dealing with an incident or a crisis. Fourthly, the BCM-plan preserves important resources and facilities. Finally, fifthly, the plan provides a solid framework to meet the guidelines that are obliged by public authorities.

Figure 9 illustrates the emerging values of business continuity management plans from different risk perspectives (Blyth 2009).

Figure 9: BCM Plan (Blyth 2009:6)

Figure 9 shows the value of an established BCM-plan in the organisation´s resilience. Enterprise resilience is influenced by four different risk categories which are financial-, liability-, physical- and reputational risk. Risk management in general could be considered a supporting component of business growth and as a result in enterprise resilience. It therefore shows much potential in the areas of mapping business threats and preparing adequate management responses for them. Besides, enterprise resilience can lead to improvements regarding the protection of the corporate interests, facilities and resources as well as increasing profits and sales.

To sum up, the development of a BCM-plan is valuable as it increases an organisation´s resilience.

The question that finally needs to be addressed within this chapter of the thesis is how success of a BCM-system is actually measured. For providing answers to this question, critical success factors regarding long-term success have to be regarded in more detail.

4.20. Long-term Success of a BCM-System

Success of a BCM-system is often measured by applying the so-called critical success factors which were established by (Järveläinen 2013).

In addition to the critical success factor *management support*, Järveläinen (2013) listed the following aspects: Organizational alertness and preparedness, embeddedness of continuity practices and external requirements. Management support is considered to be relevant for the tasks of the leading management team to integrate BCM in all business units. A long-term strategy approach can only be implemented successfully, when the importance of BCM is steadily pointing out.

Organizational preparedness or alertness is therefore one of the main parts of the management´s responsibility regarding BCM. An organisation which is familiar with different crisis or incident scenarios and has know-how regarding methods or disaster management approaches will manage negative occurring events much more efficient than others. On that account the term familiarity is significant for many businesses. The reason for this is seen in the feasibility of an organisation to recover and take on business operations after an incident –in other words: how the organisation´s resilience looks like.

The embeddedness of continuity refers to the preparedness of a company regarding their business continuity practices. Those consist of continuity methods that are implemented into business processes and the intensive involvement of all stakeholders, especially the level of staff involvement into practices for disaster recovery. The sum of these crucial components including organizational alertness and preparedness, embeddedness of continuity practices and external requirements make up an organisation´s embeddedness of continuity. Besides, the quality of the single components will be reflected when a crisis hits the organisation and it comes to light how the entire corporation will actually behave (Bakar et al. 2015b). Due to a rapidly changing micro- and macroenvironment the significant components developed and changed over time. Especially, digitalisation and the issue of big data plays a crucial role in this context. Additionally, newly emerging threats, like for example blackouts or pandemics are challenging the BCM-systems of DB, Austrian Red Cross and DPMA.

The previous parts of the thesis have shown that especially in times of crisis (e.g., Covid-19 pandemic), a BCM system´s effectiveness comes true. The BCM systems that are currently in-use are heavily overloaded due to the large amount of data. As a result, they no longer function properly.

During the expert-interviews it has been stated, that there is a strong need after a tool that improves the existing BCM systems and expands their functionalities, especially regarding the challenges of dealing with high volumes of data. There are a lot of factors that may improve the effectiveness of BCM-systems. Based on the interviews conducted it specifically came to light, that a need regarding the optimisation of internal communication process is given. Furthermore, expectations are that information could be easily exchanged between different divisions of an organisation and that tasks won´t be conducted twice due to miscommunications regarding the allocation of tasks. In addition, the creation of awareness of the employees should be gained by attracting the attention of them for the topic BCM and the highest level of effectiveness should be reached complying the capacity restrictions.

To meet the expert´s expectations and to support the BCM-systems that are currently in-use a further tool is needed.

Therefore, the knowledge graph has been identified during research which is subsequently added to the thesis. The following chapter will analyse the theory of the knowledge graph at first and afterwards moves on to the construction process of a holistic knowledge graph template that could be applied by the BCM-systems of DB, Austrian Red Cross and DPMA.

CHAPTER V.

Theory: Knowledge Graph

The current BCM-systems of DB, Austrian Red Cross and DPMA are heavily overburdened, as the data got too big to be handled efficiently. High volumes and high-speed data have become the main challenge for the BCM-systems. As a result, the BCM-systems of critical infrastructure organisations are reaching their limits and are malfunctioning and very slow regarding their operations. For this reason, processes usually take very long.

The idea of implementing an AI-based tool that could on the one side handle Big Data and on the other side generate new knowledge from interconnected data available could expand and support the BCM-systems in a certain sense. For this reason, the Knowledge Graph is added to the thesis.

5.1. Knowledge Graph Definitions

A graph that illustrates real-world entities and their corresponding relations to other entities is a knowledge graph. It shows different topical domains and categorizes various entity-classes and their relations to each other (Paulheim 2016 cited from: Ehrlinger & Wöß 2016).

„[…] systems exist, […], which use a variety of techniques to extract new knowledge, in the form of facts, from the web. These facts are interrelated, and hence, recently this extracted knowledge has been referred to as a knowledge graph" (Pujara et. al 2013)

These two definitions show that a knowledge graph (KG) is kind of a database which collects an extremely high number of data that is interrelated. This actually represent the missing key of the BCM-systems that are currently in use at DB, Austrian Red Cross and DPMA. The entire database uses various techniques for extracting new knowledge out of the available information. To sum up, the idea behind a KG is to make enormous amount of data useful, by analysing the data of different sources and the connections between them in detail and finally, creating knowledge for further use. In this context, the issue of interoperability of a KG is relevant to mention, as it allows the cooperation between different systems.

The idea of a KG network is counted among as an important aspect of the artificial intelligence (AI) technology. Within the graph, relationships of concepts are represented and described in a useful and structured way. The key tool of KG technology is to simplify massive amounts of data (Big Data), organize it and extract the actual sense and relevant connections out of it. Therefore, its ambition is to filter relevant information, that generate intelligence and value. This implies that a KG could be a possible tool to handle the big amount and high speed of data that critical infrastructure organisations currently have to deal with.

A Knowledge Graph consists of many entities which are represented in the form of nodes and their relations to each other which are portrayed as edges. An edge is built on a head entity, the corresponding relation and the tail entity. Entities are always in relation to other entities and connected to each other through the respective edge. The triple construction of facts makes KG well protected against manipulations. This is based on the symbolic nature of the triples used (Wang et al. 2017).

There are various techniques than could be applied for the triple construction process. A characteristic embedding technique comprises three steps: the initial presentation of the entities and their

corresponding connections in a certain vector space, the definition of a scalable feature and the learning component which strongly relates the subject KG to the issue of AI (Wang et al. 2017).

AI is considered state-of-the-art, especially concerning the construction of a KG. However, even before the issue of artificial intelligence was widespread and well-known the idea of knowledge sharing was already born.

5.2. Knowledge in 1991: The Vision of Knowledge Sharing

Neches et al. (1991) highlight impediments considering the sharing and reusing aspect of knowledge. To sum them up, the biggest obstacles are found in the heterogeneous representation, dialects within the language families, the lack of communication conventions and model mismatches at the knowledge level.

Every situation requires a different approach of knowledge representation. While one model of knowledge presentation could be very efficient in one situation, the same formalism is not adaptable and can therefore not be integrated to another formalism. This implies that there is no single knowledge representation that is suitable for all kind of problem scenario.

Another barrier to reuse knowledge are dialects within language families. If knowledge has been encoded by applying diverse syntax and semantics, using or sharing same knowledge patterns across various systems is difficult.

A third impediment concerning the problem of knowledge sharing is seen in the lack of communication conventions. This is based on the idea of connecting different knowledge bases by communication. By connecting two knowledge bases through information exchange, both systems can benefit without merging knowledge bases.

Finally, the mismatches at the knowledge level of a model became a subject of discussion. Even if the language dialects barriers have been overcome, there are further issues like for example the type hierarchy of knowledge bases. One system may design the structural arrangement of objects differently from another knowledge base. While one system segment objects into the categories physical- or abstract object, another base may be structured completely different. These differences are often reflected in the different purposes of the individual knowledge bases and are difficult to reconcile for the reasons mentioned above.

Although, there are various impediments which still have to be overcome, Neches et al. (1991) discussed the vision of knowledge sharing already in 1991. The initial assumption was that future knowledge bases shall be constructed by assembling reusable components in form of a modular systems. The idea was that rich knowledge bases will be established from time to time. By sharing problem-solving techniques or explicit knowledge among different knowledge bases, intelligent systems will emerge. In addition, to many other advantages and benefits that arise from the use of these intelligent systems, the resilience of the systems will also improve due to the repeated reuse of well-tested components (Neches et al. 1991).

The following paragraph will analyse the issue of the connection between knowledge and AI in more detail.

5.3. The Connection between Knowledge and Artificial Intelligence (AI)

Since the late 20th century scientists more and more realize that knowledge is considered to be the key element of AI-systems. The difficulty is to represent the knowledge in a meaningful manner. This step

is costly and in particular extremely time consuming as every knowledge base has to be built from scratch. This means that there are no pre-developed tools which could be applied to different kind of knowledge collections. This was also the reason why knowledge-systems developed at first (within the late 1970ies) only consist of a relatively small number of data (knowledge-components). Therefore, a key issue for the development of more significant AI systems was to establish a tool which has features to preserve knowledge and allows to build on the existing knowledge bases and refine them.

Nowadays, in 2021 there are various modes of reusing data and methods for building on existing databases. For instance, the exchange of various techniques presents one possibility type for the reuse of data. This implies that a specific module which is stored in the "knowledge-library" is re-applied by adapting the module and solely using the concept behind the module. Another way in which pre-existing data could be reused is through the integration of source specifications. By copying one module´s content into another framework, further processing could be conducted. While the two modes of reuse represent adequate options for the subsequent use of data and therefore a possibility to let AI systems grow, they are not particularly suitable tools considering the expansion of knowledge databases in the 21st century. This is inter alia based on the fact, that a common understanding of more than one data set is often required when reusing certain kind of data. It is precisely the aspect of common and shared understanding of data that receives inadequate attention for today's complex scenarios and interfaces of data (Neches et al. 1991).

> *"Primary reasons for the popularity of KGs in this century are: enabling new generation of applications for (prefacing with "semantic") search, browsing, recommendation, personalization, advertisement, etc. - both for the open Web as well as enterprises, and enhancing already very popular AI techniques of machine learning and natural language processing (NLP)."*
> (Sheth et al. 2019)

Based on the fast increase of the number of Web users since the 1990ies, the "search-feature" got of immense importance in societies all over the world (Sheth et al. 2019).

Especially, when IBM implemented their AI-based platform IBM Watson a new level of coverage and popularity was reached. By the help of IBM Watson, future events could be predicted (IBM 2021). Considering critical-infrastructure organisations BCM-systems making forecasts, for instance like the procedure of a crisis that hits an organisation could be very useful. Processes run automatically and simultaneous to each other and thus can be optimised. In this context the term interoperability plays an important role because systems like for instance IBM Watson strive to recognize connections between different sources and components within a platform (Sheth et al. 2019).

5.4. The Concept of Knowledge Bases

A knowledge base is a method to store different kind of large data repositories and to prepare structured as well as unstructured information for a further implementation to a knowledge graph. Knowledge bases and knowledge graphs are strongly interrelated. However, the tendency of a KG is more in the direction of illustrating the relations and connections between the individual entities. (Neches et al. 1991).

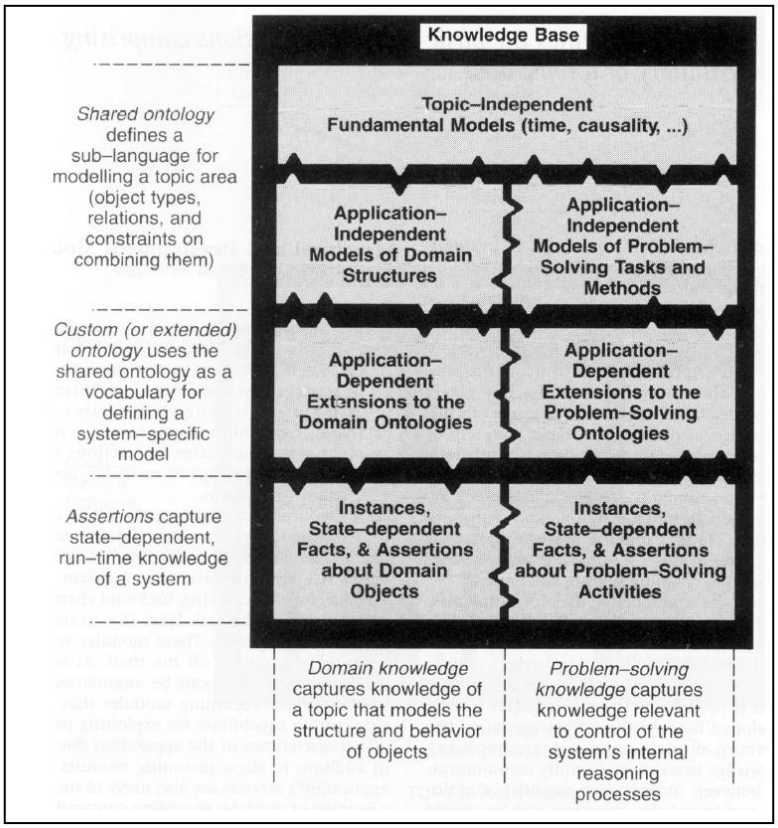


Figure 10: The Anatomy of a Knowledge Base (Neches et al. 1991:41)

Figure 10 illustrates the concept of a knowledge base and highlights the single stages regarding its anatomy. Ontologies are situated at the top of an application system. The ontologies which are considered as representational choices, consist of topic independent as well as topic-relevant information. In the next stage a more application-specific model is compiled. The ontology on top and the more specific consideration together make up how a special application illustrates an issue. At the bottom-line statements are made by gathering the available knowledge of the system. Figure 10 shows that information in the form of knowledge at the bottom level is more specific than at the top. Less specific knowledge is simpler to share and to reuse than specific know-how. However, the possibility of sharing more specific information is not impossible. In the case that a system accepts the models in the higher levels, knowledge can be exchanged and repurposed (Neches et al. 1991).

5.5. The Benefit of Knowledge Libraries

The concept of knowledge bases showed that the visualisation of a scenario, like for instance a certain crisis situation was simple and clear, and mostly suitable for only one complex situation. While ontologies were divided into specific and less specific information, there was no possibility to collect certain knowledge. The implementation of a knowledge library which collects and stores information expands the model.

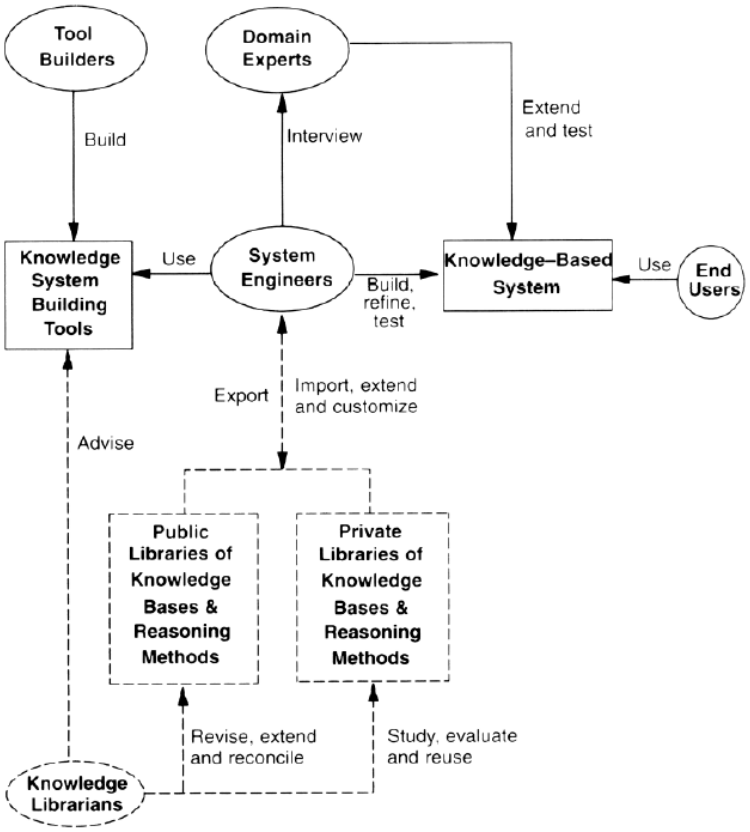


Figure 11: Current versus Envisioned Models of the AI Software Life Cycle (Neches et al. 1991:45)

The current versus the envisioned model of the AI-Software-Life-Cycle is shown in figure 11. Basically, the model consists of four main participants: Tool builders, system engineers, domain experts and end-users. Tool builders cover the process to build knowledge system tools. Afterwards the system engineers apply those tools developed for constructing knowledge-bases by receiving input of the domain experts. Furthermore, those two participants (system-engineers and domain experts) fine-tune the systems by conducting tests or extensions. Lastly the end-users activate the system.

As figure 11 shows a further component has been added to the system –knowledge libraries. Those could cover two types of knowledge –a structural and a problem-solving one. The incorporation of libraries brings major changes to the functionalities of the system, as now submitted data in form of ontologies and logical formalism are efficiently enough prepared for conducting operating tasks. By providing a variety of modules within the library, major advantages considering the construction work process result. Even tool designers will benefit by the development of system-specific tools and the designing-process which supports the core activities of the system.

To sum up, the implementation of a library to the system brings great benefits and a significant change regarding the methodology for the construction process of a knowledge base. The libraries could be further extended to the BCM-systems of critical infrastructure organisations. The implementation of a library that covers structural and problem-solving knowledge could improve the current systems by generating ontologies and to make more relations between the components of the BCM-systems visible. Furthermore, it could enable the possibility that a KG is applied to different scenarios.

In this context, there are various applications of a KG, like for instance the KG of the technology company Google. The following section will give a brief overview of KG real examples.

5.6. Knowledge Graphs - Examples

The main KG in these days is presented by Google. The search engine represents the most-known and most innovative KG. (Uyar und Aliyu 2015) Basically, the term knowledge graph referred exclusively for Google´s Knowledge graph (Bellomarini et al. 2018a).

The idea behind the search platform was to provide answers to customer´s queries. Google act as kind of an intermediate between the users on the one side and the papers and documents provided by the world wide web on the other side. While this actually has been the basis idea behind search engines, the developments went into another direction. Search engine platform providers wanted to understand the user queries semantically. If, in this case, search queries are understood precisely, the serving of the requested information will be much more concise. The final aim was to provide the required information from Google´s knowledge repositories (Wei et al. 2020).

Nowadays, besides Google, other giants, like for instance Alibaba, one of the largest B2B trading platforms worldwide, the online mail-order company Amazon or the social-media network Facebook, make use of knowledge graphs (Bellomarini et al. 2018a).

5.7. Three Components of the KG-Concept

The concept of the KG has been divided into the following components: the artificial constructed knowledge resource, the construction on swarm intelligence and data is taken from internet link data. The artificial component means that "early knowledge" has been manually added and edited in the graph, like for instance in the case of the semantic network WordNet (Fellbaum 1998 cited from: Wei et al. 2020).

Data within the KG is built on swarm intelligence. Swarm intelligence is situated in the area of artificial intelligence and rests upon the collective behaviour of elements in centralized- as well as decentralized systems. Additionally, it is closely related to ioT, especially in the decision-making process regarding complex scenarios. (Rath et al. 2020) The third component refers to the Linked Open Data (LOD), a project that is following an open-source approach. On this occasion the aim is to use highly innovative technologies for the implementation of recent knowledge (Swarm intelligence for resource management in internet of things 2020).

Excursus: Ways of Knowledge Representation

There are various ways to represent knowledge. In addition, there are also different encoding techniques considering the translation of information to a specific system. The *distribution representation* is one of those. It mostly consists of words and phrases. The process follows the following procedure. The embedding technique tries to understand and analyse low-dimensional vector statements of large data. The outcome –the learnt knowledge is implicit. Besides the distribution representation, there is a more structured representation for knowledge, which is shown in the model of a semantic network (Chen & Xiao 2020).

In order to provide the reader a better understanding of the representation of knowledge within a KG, it is relevant to take a closer look at the so-called groundwork theories of the KG. The theory of the KG is not only based on one basis theory. Actually, there are three groundwork theories that need to be

considered. Therefore, the following part of the thesis will take a closer look at the relational model by Edgar Codd, semantic networks and the concept of ontologies.

5.8. Representation of Knowledge: Relational Model, Semantic Networks, Ontologies

Theory of the KG is based on various other theories. The Entity Relationship Model (ERM) by Edgar Codd, the theory of Semantic Networks and the idea of Ontologies are the main groundwork for the emergence of knowledge graphs. The following paragraphs present the basis of these theories in more detail.

5.8.1. Entity Relationship Model by E. Codd

The Entity Relationship Model (ERM) by Edgar Codd is considered as a key technique regarding the modelling process of information technology systems. The ERM makes various information structures of an issue visible. This is achieved by defining entities and their connections. One of the main advantages of the so-called relational view is that it creates

"a sound basis for treating derivability, redundancy, and consistency of relations."

(Codd 1970)

Besides, the relational model provides more clarity regarding the extent and limitations of data that is provided within a system.

However, Codd´s (1970) relational model shows many advantages of representing entities, the possibilities of illustration are limited. For instance, data in Codd´s system cannot easily be changed or adapted. This is based on the limited data dependencies within the models. The result is a disadvantage regarding the flexibility of changing entities.

In addition, the relational model is often confusing due to its overload concerning the representation of collections of data. Therefore, three kinds of dependencies still have to be eliminated. The three kinds are: ordering- indexing- and access path dependence. Since the three kinds of dependencies are not relevant at this stage of analysis, they will not be discussed further here (Codd 1970).

Codd (1970) defines the key success factors for a relational database on the basis of the data quality, the storage capabilities, transactions, service and the data query.

5.8.2. Semantic Networks

Semantic networks are a popular knowledge representation formalism.

Bell et al. (1969) deals with the issue of semantic memories. They present a tool for the modelling of cognitive relations. The so-called memory model represents a format for the organisational arrangement of information and the structural illustration of data. The model serves as a proposal for the logically transferring-process of a large amount of data in a computer. The approach of the memory system is to represent knowledge in form of concepts but only in a descriptive way. This is how Bell et al. (1969) attempt to depict real world scenarios from an objective and fact-based point of view. The aim is to leave any subjective perceptions and all kind of emotional perception out. The entire memory is illustrated in knots which represent entities and their belonging relationships. The real approach is to

understand the entire system, especially the interrelationships between the knots that stand for a specific connection. For the mapping of an explicit system, all nodes (concepts) that are in touch with other entities shall be connected by lines, so that all dependencies are captured. A further aim is to show hierarchical relationships between different subjects (Bell & Quillian 1969).

The following extract shows a simple representation of a semantic network graph which is properly structured, by visualising the interrelationships and the relationships between the individual entities.

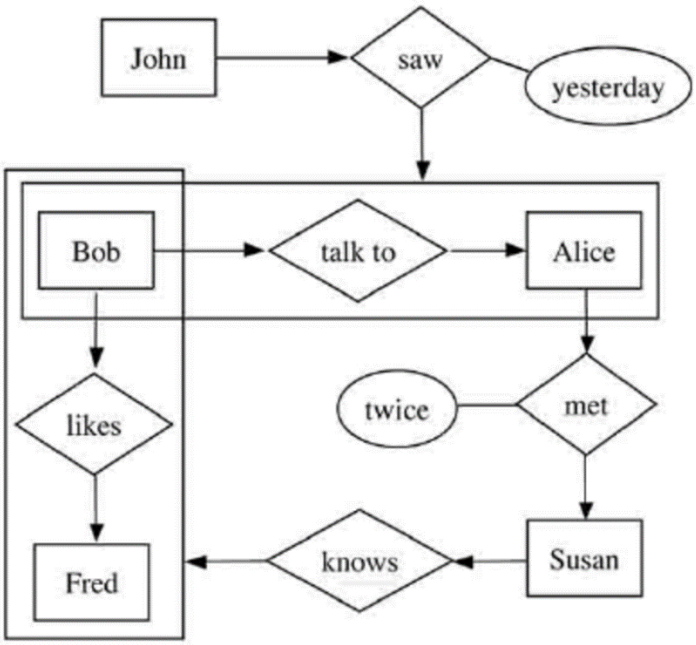


Figure 12: A simplified Semantic Network created from the sentences (Harrington & Clark 2007)

A semantic network constitutes a framework for the implementation work by a data scientist or an engineer to a computer system.

Semantic networks got more and more innovative and popular over the last decades. However, WordNet or other traditional semantic networks are bounded by a certain number of relations. (Miller 1995 cited from: (Chen und Xiao 2020) Since, the number of data continuously grew, and the proliferation of these large-scale data networks got closer attention, the term `knowledge graph´ was created. (Bordes & Gabrilovich 2014).

Noteworthily projects to mention in this context are the knowledge graph DBpedia, Wikidata or BabelNet (Chen & Xiao 2020 cited from: Qiao & Hu 2020).

The reason for the explicit knowledge extraction out of the various amount of data, is seen in the graph´s semantic processing capabilities. Therefore, the theory of semantic networks is considered as one of the basis theories for the KG (Wei et al. 2020).

Well-developed semantics could constitute an ontology which is a more structured representation concept. (Gruber 1993) Therefore, the concept of ontologies is considered to be another relevant

groundwork for the theory of the knowledge graph. The concept of ontologies is analysed in the following paragraphs.

5.8.3. Ontologies

The key approaches and procedures of a KG, show similarities to the language of ontologies. Common features are for instance seen in the relationship extraction, knowledge representation, fusion methods or the entity learning (Wei et al. 2020). Besides, also knowledge bases consist of ontologies (Neches et al. 1991).

The following paragraph provides more insights what ontologies are actually about.

An ontology is understood as a formal description of approaches and their connection to other concepts. That means, that ontologies solely consider the character and the structure of an object. The description of ontologies is made in terms of general properties of the object itself and its relation or connectedness to other items. There are various definitions of ontologies, however, in this context the thesis focuses on ontologies which are designed for AI systems, like for instance computational science. In this context, an ontology is described as follows:

"*a special kind of information object or computational artifact"*

(Guarino et al. cited from: Staab & Studer 2004:2)

So-called computational ontologies are responsible for the structural development regarding the creation of a model. To sum up ontologies are applied as kind of a schema-layer for the representation of information in knowledge-based systems.

Conceptualisations in the form of illustrations of entities and their relations play an important role regarding the visualisation of real-world phenomena for the creation of computational ontologies.

According to Borst (1997) an ontology is a

"formal specification of a shared conceptualization"

(Guarino et al. cited from: Staab & Studer 2004:2)

Borst (1997) firstly mentioned the importance of the concept of sharing. He understands conceptualisation as the expression of a common view expressed by several parties involved. The focus of conceptualisation of ontologies is therefore seen within the collective expression of a perspective, rather than the individual view (Staab & Studer 2004).

Conceptualisations are specified either extensionally or intentionally. Due to the continuous listing of extensional scenarios (all possible relations of an object), the extensional conceptualization is unsuitable. Hence, it makes more sense to draw conceptualisations in an intentional way and to determine a language that shows constraints instead of indefinite scenarios. Therefore, ontologies are understood as explicit definitions in the context of conceptualisations (Staab & Studer 2004).

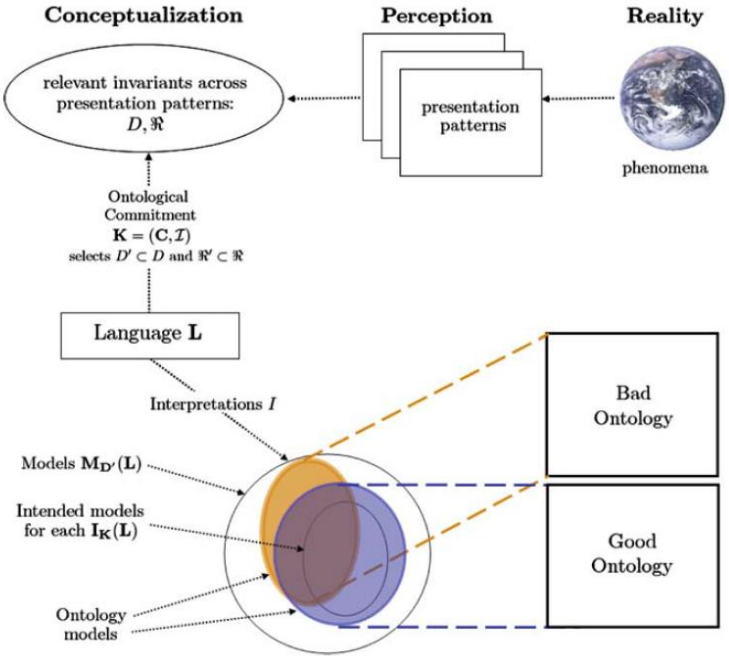


Figure 13: The relationships between phenomena occurring in reality, their perception (at different times), their abstracted conceptualization, the language used to talk about such conceptualization, its intended models, and an ontology (Guarino et al. 2009)

Figure 13 summarizes all the components and their relationships for the construction of an ontology. This constitutes the missing key in the BCM-systems that are currently in-use at DB, Austrian Red Cross and DPMA. Due to the high amount of data too little significant connections become visible. This leads to the status quo which is characterized by an inefficient system.

The result, which is based on the qualities of inputs of figure 13 is seen in a good or bad ontology. (Guarino et al. cited from: Staab & Studer 2004). In this sense, Gómez-Pérez (2004) categorizes between ontology verification and ontology validation. The verification refers to the correct creation of the ontology. This means, for example, using an appropriate language to ensure that the requirements are implemented correctly. Validation refers to whether the phenomenon actually corresponds to the real world and has been correctly mapped within the ontology. In summary it can be said that verification deals with the question whether an ontology has been constructed correctly, while validation in comparison observes the issue from a more general perspective and answers the question whether the correct ontology has been used for the mapping of real-world scenarios. (Gomez-Perez 2004 cited from: Staab & Studer 2004).

According to (Gruber 1993) a main issue when implementing ontologies is the problem of portability. The major challenges in respective to a commonly created ontology, designed by more than one party, is seen in the fact of different languages that are applied. Due to the fact that, different applications require different argumentations, a language should be scenario-specific. Therefore, it is not useful to implement a standardized language to a system. By the application of a translation approach Gruber (1993) presents a tool for the translation of ontologies. By the creation of knowledge-based systems, the implementation of a software engineering method, that is built on technical specifications of shared resources is relevant. Thereby, the choice of accurate (a common) vocabulary within the methodology is of great significance.

Therefore, interoperability is a core requirement for an AI-capable knowledge-based system. The ability of collaboration is understood as the permanent exchange of information within the system. Three conditions emerge, that are indispensable for the proper operation of the collaboration aspect. Those consist of the selection of an adequate language format in the sense of precise knowledge representation, an agent-based communication protocol and finally, the specification regarding the substance of joint know-how (Gruber 1993).

5.9. Conceptual Knowledge Processing (CKP)

Conceptual Knowledge Processing (CKP) is considered a method that that seeks to the creation or identification of methods that could be applied for the processing of knowledge. Moreover, the processing instruments developed should support human thinking, acting and judging in a rational way (Wille 2006).

A further definition of CKP is the following.

"Conceptual Knowledge Processing is considered to be an applied discipline dealing with ambitious knowledge which is constituted by conscious reflexion, discursive argumentation and human communication on the basis of cultural background, social conventions and personal experiences."

(Wille 2006)

While the term "conceptual" in CKP relates to the constitutive function of a human being arguing, acting, or thinking, the term "processing" refers to a situation in which something is produced or gained in the form of knowledge. This means that knowledge that derives from human minds has to be represented in a formal way. This is a basic condition behind the idea of conceptual knowledge processing.

"According to pragmatic philosophy, knowledge is formed in an unbounded process of human thinking, arguing and communicating; in this connection, reflection on the effects of thought is significant and real experiences stimulate re-thinking time and again. In this process, form and content are related so closely that they may not be separated without loss."

(Wille 2006:2)

Basically, CKP is based upon a formal mathematical logic and its mathematical quintessence rests on the formal concept analysis. Formal concept analysis consists of the idea to include all of the in- and extensions that are represented. In this context, the extension stands for all further subjects that are falling under the concept and the intension is related to the joint features of the object. To sum it up, conceptual knowledge is composed of a collection of objects, their properties and features and the relations that connect an object to an attribute (Wille 2006).

Considering the BCM-systems of DB, Austrian Red Cross and DPMA, the CKP represents a method that could expand the present systems by the processing of knowledge from data available. CKP is one possibility to gain knowledge out of information available. In addition, it could be further used for the construction process of a knowledge graph for the BCM-systems of the critical infrastructure organisations interviewed. The following section provides an overview of the construction process of a KG.

5.10. The Construction of a Knowledge Graph

Knowledge-based systems are constructed on two components: the knowledge itself (the information in form of data) and the so-called inference-engine which is among other things able to identify new facts or findings by answering questions with the help of knowledge available. (Akerkar et al. 2010 in Fensel et al. 2020:4) Furthermore, the knowledge base consists of two different kinds of boxes: ABox and TBox. While an assertion box (ABox) is composed of a chain of facts, a TBox, the terminological box deals with the terminology that is further applied in Abox. (Brachman & Schmolze 1985)

The construction process of a KG could be summarized in four steps. These steps consist of: the knowledge creation, the knowledge hosting, the knowledge curation and the deployment of knowledge (Fensel et al. 2020).

Gómez-Pérez et al. (2017) state that for the creation of a knowledge graph components like the knowledge representation and reasoning, the safekeeping of knowledge (the storage of data), the applied methodologies (knowledge engineering), the AI component of knowledge (knowledge learning) are highly relevant to consider (Gómez-Pérez et al. 2017 cited from: Fensel et al. 2020).
The following figure illustrates the individual components that in total make up the generation of a knowledge graph.

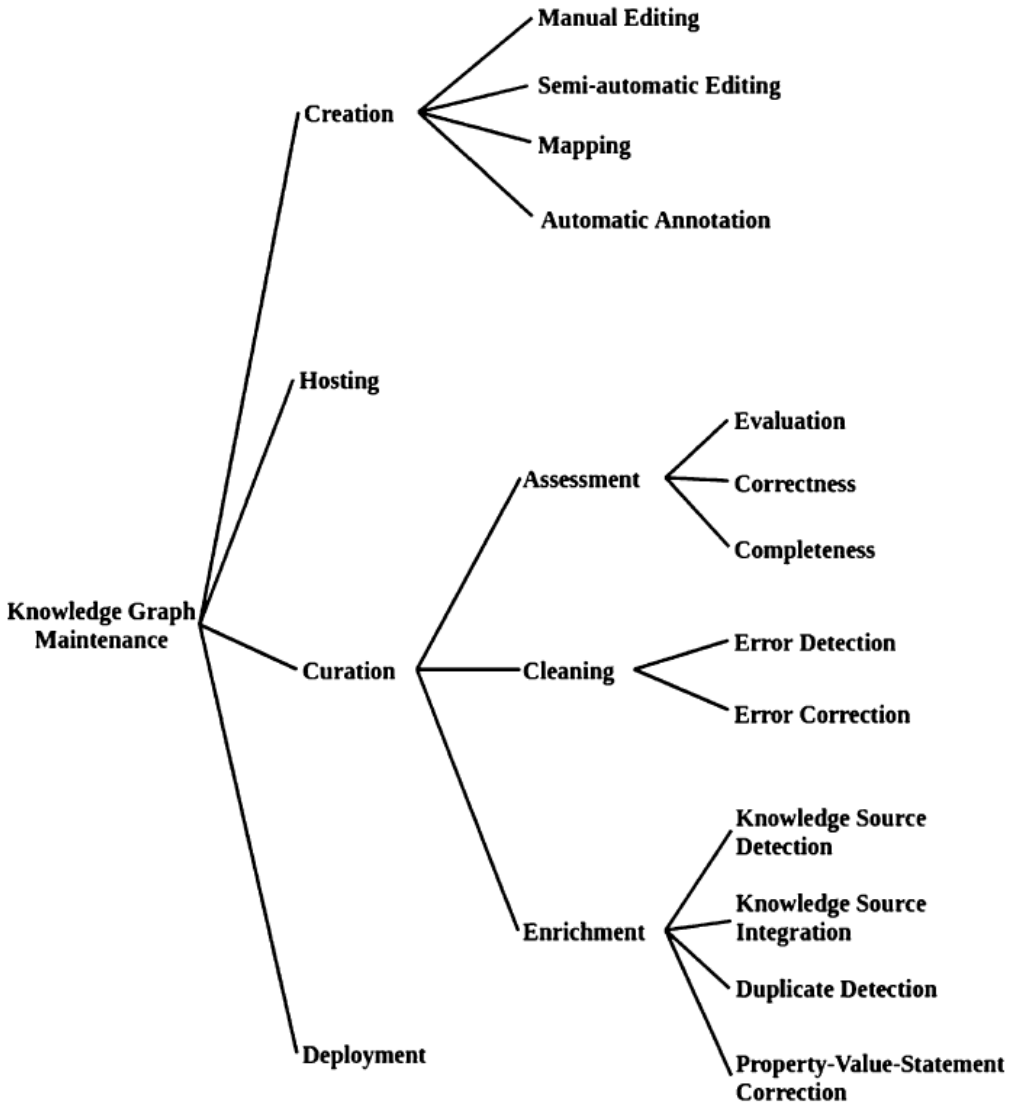


Figure 14: Knowledge Graph Generation (Fensel et al. 2020:26)

The learning capability represents a key function regarding the construction process of a KG. This is ensured by the application of machine learning algorithms (Sheth et al. 2019).

5.11. The Application Process of KG

Through the years the application of the KG has wide spread. The scope of application is big from question answering- or recommendation systems to medical support frameworks which deliver required information that is highly precise (Wei et al. 2020).

The thesis already showed that the KG utilizes triples, for the representation of facts. The triples consist of entities, their relationships to other entities and various concepts (inter alia properties and the corresponding values to the properties). Entities are considered to be the most basic element within a KG. An entity represents an object that has an unlimited number of connections to other entities. Concept stands for different categories or types of objects and the properties mainly refer to the specific

characteristics or features an object might have. Finally, the value of the attribute is related to the actual value of the unique property of the object (Wei et al. 2020).

Therefore, the KG is considered a possibility to describe these complex problem statements by presenting entities and their interconnected relationships to each other. (Wei et al. 2020) Concerning the BCM-systems of DB, Austrian Red Cross and DPMA, the KG could be considered as a tool that shows the most important entities and their relations to each other. The finalized KG that covers the BCM-systems of the critical infrastructure organisations that have been interviewed could be applied to different crisis scenarios. As a result, the course of a crisis within the BCM-system and the affected areas could potentially become visible.

According to Sheth et al. (2019) a KG can be utilized for distinct forms of data processing and management tasks. This approach could be further applied to improve data processing of BCM-systems. In this context, the application of a KG, search-, browsing-, data integration- functions that are collected from different sources should be improved. Thereby the focus is the semantic approach.

Considering the application of a KG someone can distinguish between knowledge graphs and knowledge networks.

> *"Knowledge Networks (KN) integrate and combine knowledge (usually captured as KGs) from various domains. Knowledge networks should have schemas, datasets, and documentation to explain their usability across applications, and provide "horizontal services" to support knowledge-intensive applications, and may specialize to focus on a chosen domain (i.e., "vertical KN", as in neuroscience KN), and interconnect multiple fields to create a cross-domain KN."*
>
> (Sheth et al. 2019:2)

The semantic approach that is followed is also relevant for the creation of knowledge because it addresses the problem regarding the missing data uniformity. Especially regarding the construction of a holistic KG for the BCM-systems of DB, Austrian Red Cross and DPMA consistent data is significant for the information value of the KG. However, data has to be organized for instance according to the triples-principle by Wei et al. (2020).

5.12. Creation of Knowledge

Knowledge creation describes the process of information collecting via different sources. Knowledge is represented in different ways, including text documents, videos, databases, etc. The fact that knowledge is represented in various ways, is kind of a problem as there is no data-uniformity regarding the graph-implementation process. One way of overcoming this barrier is seen in the application of semantic data which is a methodology that will be analysed in more detail within the following paragraph.

In the first step of the knowledge creation methodology, the aim is to identify a specific domain area. Subsequently, the selected domain is analysed with regard to real-world entities and their interrelations. The next step that follows is the analysis of the online representation of single entities. Special attention is paid to the type of data. The analysis of the online representation, is the first approach to understand and categorize data. The aim is to identify the kind of data that is relevant for the creation of the annotation process (Fensel et al. 2020).

5.13. Knowledge Graph Management System (KGMS)

Knowledge of a KG consists of a few variables, which are mostly big data volume of corporate as well as public sources and rule-based know-how. An enterprises KG has to contain relevant business

information, for instance the client base, the competitive situation, products and their corresponding prices, etc. All of this is managed in a so-called knowledge graph management system.

As the equation shows a KGMS consists of the knowledge base management system (KBMS), which is the component that is responsible for the rule-based reasoning processes that is made out of the big data volume. The big data volume applies AI tools, like machine learning or methods of data analytics to the information collected. This exactly represents the requirement expressed by the experts regarding a tool that expands the BCM-systems that are currently in-use at DB, Austrian Red Cross and DPMA. An application of an AI-based tool to the huge amount and high-speed of data that challenges BCM, could lead to an improvement of the systems.

Nowadays many organisations try to get the most out of the knowledge they gather. By collecting data and automatically letting the information flow to an organisation´s knowledge graph, many companies strive for the ability to manage their knowledge by applying a KGMS. This kind of framework provides a lot of benefits for an organisation, as it is able to manage difficult and complex reasoning tasks, handle the issue big data and generate intelligent deductions from the data collected, like for instance the generation of relations between specific data. While on the one side KGMS are intelligent systems which generate great value for whole organisations, on the other side they require the right kind of input variable. For linking and comparing data in a useful way, KGMS need interface functions. In more detail, KGMS connect large databases to AI functions, like machine-learning, the web and analytical methods.

Figure 15 will show some architectural-aspects regarding the structure of a KGMS.

Starting point of a KGMS is always its “core reasoning” which is the component that is responsible for the creation of rule-based knowledge. In other words: it represents the key part that has profound insights to the set of rules and rule repository of the entire graph.

The circle outside the central area shows different modules which are all tools for gathering or accessing data, like for instance the control language SQL. For providing proper and useful information, the reasoning core has to apply a specific language for the KRR –the knowledge representation and reasoning. It is relevant that the selected language meets the demands of finding a compensation regarding the relation between complexity and expressive power.

VADALOG KGMS for instance, is a language that shows functionalities that balance these two characteristics smoothly. VADA stands for Value Added Data Systems. The VADALOG KGMS applies the VADALOG language to various methods from databases and AI practices, like for instance the dynamic in-memory indexing.

The outermost circle demonstrates components inter alia ioT, Relational Database Management System (RDMS) or data that is represented in network structures, like the Graph DBMS, that are all characterized by their analytic features (Bellomarini et al. 2018b).

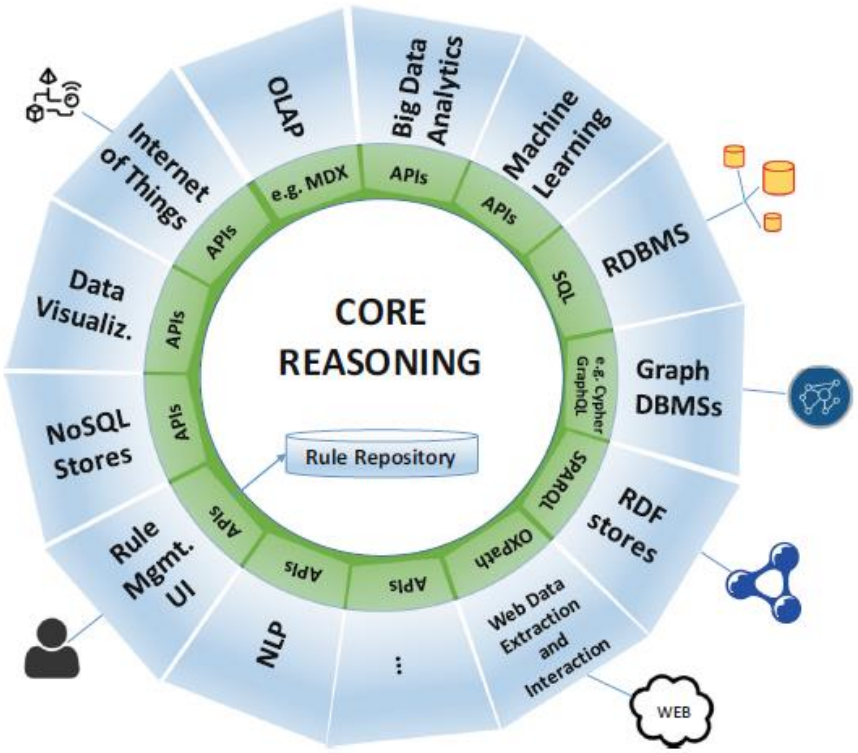


Figure 15: KGMS Reference Architecture (Bellomarini et al. 2018b)

Figure 15 illustrates how a KGMS looks like and of which individual components it consists. The KGMS Reference Architecture could be further used for the construction of a KG for the BCM-systems of the critical infrastructure organisations that have been interviewed for the thesis. Knowledge flows within the BCM-system could be efficiently managed with a KGMS.

For the construction process requires some preconditions which are analysed in the following paragraphs.

5.13.1. Requirements for the Construction of a KGMS

Although a KGMS is made up of many small components that all contribute to the effectiveness of the entire management system, three core areas emerge:

- the selection of logical formalism (language)
- the collection and management of big data
- procedural third-party code.

The following paragraph will analyse these sections specifically.

5.13.1.1. The Selection of Logical Formalism

In order to guarantee the efficient functioning of the core reasoning, it is important to define a uniform language for the KGMS. During the definition process of an accurate language, it is important to take care of the features concerning simplicity and a modular syntax. Besides, rules of logic programming

should be especially considered, like for instance the fact that data should match database tuples. Besides, the attribute of high expressive power is an important feature that the selected language should demonstrate. The rule language should produce strong and clear fact-based statements. Furthermore, for the creation of logical formalisms a further attribute of the language selected is the efficient handling of numeric values. The language system should highlight the ability to put probabilities to the corresponding reasoning process. In this process, facts are given certain values that are newly evaluated time and time again. Changes or adaptations in this regard should be therefore easy to adjust. Additionally, rule language should be provided with ontological reasoning as well as a low level of complexity. Especially, the requirement of low level of complexity for the language applied is essential, when the KGMS is recognizing rule sets. In order to anchor the rules of a system in an ideally structured and detailed way, a kind of rule management is required. This could be done in the form of a collection of different rules within the scope of a library. In this context, a system has the ability to store already-known facts and access those easily. In this sense, an ontology editor is very reasonable. Finally, for extremely large amounts of data, a master module has to be implemented as the management of the high volume of data gets too complex (Bellomarini et al. 2018b).

5.13.1.2. Gathering and Managing Big Data

Besides the selection of the optimal KGMS-language, the issue of the missing consistency within data available plays an important role. In this sense, it is necessary that the system connects the accurate sources of data in a meaningful way. In addition, the system should be able to sort out irrelevant data which should not be implemented to the main-memory of the KGMS. Regarding the size of data set, decisions should be made on whether to integrate data processing tools into the system or not. Furthermore, it should be ensured that one has access to databases and data warehouses, such as RDF (Resource Description Framework) stores.

According to Bellomarini et al. (2018) the implementation of an Ontology-Based Data Access (OBDA) is valuable. The implementation of OBDA enables the system to conduct a request which has been created at the head of an ontology. For the creation of useful ontologies, the quality and quantity of data are of crucial importance. Integrating the required data, exchanging and removing it from a system is the prerequisite for ensuring a certain quality level. This can be put into practice by applying an appropriate KRR (knowledge representation and reasoning) method to the system. In conclusion, the KGMS should be in conjunction with the web (Bellomarini et al. 2018b).

5.13.1.3. Procedural Third-Party Code

Finally, the third component considering the requirements for building a KGMS: the third-party code. A procedural code is understood as an included application that consists of procedural code that is recorded in various programming languages. Additionally, the implementation of useful packages, provided by third parties, like for instance Text Mining, NLP, Data Analytics or Machine Learning could bring previously unavailable benefits to the KGMS (Bellomarini et al. 2018b).

5.14. Datalog & Vadalog

There are three basic conditions for the reasoning of knowledge graphs.

1. Recursion Capabilities

The capabilities to recursions enable the facilitation of complex tasks within a KG. Navigability concerning the connection or separation of different tasks or a single presentation of a problem are necessary for efficient graph-based structures.

2. Formation of Ontologies

The construction of ontologies constitutes one of the major background theories on which a KG is built upon. At any rate, ontologies should present reasoning, which implies that new, additional information is generated from available data.

3. Low Level of Complexity

Finally, the level of complexity. Huge amount of data shows a high level of complexity, especially when data is raw, not filtered or structured at all. Therefore, reasoning within a KG has to be steerable as well as comprehensible. This is a prerequisite for the following scalability (Bellomarini et al. 2018b).

"DATALOG is a declarative (programming) language. This means that the programmer does not write a program that solves some problem but instead specifies what the solution should look like, and a DATALOG inference engine (or Deductive Database System) tries to find the way to solve the problem and the solution itself. This is done with rules and facts. Facts are the input data, and rules can be used to derive more facts, and hopefully, the solution of the given problem."[7]

VADALOG, a project released by Oxford University, University of Manchester, Edinburgh and industrial partners, for instance like Facebook, BP, etc. The VADALOG system represents a programming language, that is constructed on the foundation of Datalog± and Warded Datalog± which both constitute declarative programming systems (Bellomarini et al. 2018). By comparing Datalog± and Warded Datalog±, the difference is that Warded Datalog± represents a "a high-performance Datalog± system utilising an aggressive termination control strategy" (Bellomarini et al. 2018b).

The stone of VADALOG is an algorithm, that enables high performance on the one- and finite memory storage capabilities on the other side. The question that is posed in connection with the finalization of the development of the algorithm, is related to the architectural implementation. The VADALOG system is embedded in a pipeline architecture which consists of pipes and filters. This architecture style is based on pipes, that show coherent consequences and enable logical inquiries (Bellomarini et al. 2018).

The pipeline architecture is based on four steps. It starts by the application of a logical optimizer which is a toolbox of rules. Logic transformations, like for example the deletion of redundancies or useless linkages between nodes are utilized for the adjustment of the elementary and complex set of rules.
In the following step the logic compiler transforms the norms and guidelines, provided by the logical optimizer and creates an access concept out of the information received. This concept is based on a pipeline, in which each rule is related to a specific filter (like for instance an entity).
The penultimate step of the process within a pipeline architecture is called the execution optimization. The execution optimizer is responsible for the proper functioning by optimizing the access concept in a number of ways, such as the rearranging of the chronological orders of the objects in the access plan or the adaptation regarding the ranking of forecasts.
Finally, the query compiler takes on the task of transforming the developed access concept into a reasoning query plan that shows qualitative features, like adding new values to the system or generating projections (Bellomarini et al. 2018b).

In summary of the chapter, it can be stated that a KG represents a possibility to tackle the issue of BCM-systems data overload. By visualizing real-world entities of different types and the creation of intelligent

[7]https://www.dbai.tuwien.ac.at/proj/dlv/tutorial/ (03.08.2021)

relations between the entities it could organize the currently unstructured data of the BCM-systems at DB, Austrian Red Cross and DPMA in a meaningful kind.

Due to the desired improvement of the critical infrastructure BCM-systems, which is expressed by the experts, a knowledge graph (KG) will be implemented in the following part. The initial approaches for an innovative holistic KG template, that expands the BCM-systems of Deutsche Bahn (DB), the German Patent and Trade Mark Office and the Austrian Red Cross will be illustrated.

CHAPTER VI.

Development of an "Inner-Critical-Knowledge Graph" Template
for the BCM-Systems of Critical Infrastructure Organisations

6.1. Knowledge Graph Characteristics

The following paragraphs strive to set guidelines regarding the initial approach for the development of a holistic knowledge graph. Therefore, the thesis provides basic conditions and illustrates features of how a potential KG may look like, that could be afterwards used as kind of a template for the implementation to critical infrastructures organisation´s BCM-systems. The experts-expectations which are in some sense understood as the specific characteristics that a KG has to cover, are presented within the following paragraphs.

The expectations of the expert-interviews show that one of the main deficits of the BCM-system that are currently in-use is that data is not evaluated holistically. The prerequisite for an improved BCM system is a holistic consideration of all critical processes and resources which are based on holistic evaluations regarding data that flows into the KG. When data is implemented to a KG, it has to be guaranteed that the described aspect of a holistic evaluation is met. This is due to the fact that the graph can only guarantee efficient decision-making support to a BCM-system when data is equally evaluated. The results of the uniform data assessment will be remarked as more beneficial and efficient due to the arising comparability. In general, results will be more significant when collecting and evaluating data holistically.

- ➔ **Data has to be evaluated holistically.**

The availability of data is very relevant. The question of which central databases should be used or which knowledge database the own BCM-system should provide is another relevant component regarding the characteristics of a KG.
Furthermore, the connections of corresponding data have been considered as a significant component that has an impact for the further success of a KG implementation.

At DB for instance, there are various databases that are currently in use. Although, there are inventory lists or object databases, they are not linked to each other, which leads to a large gap in terms of interrelationships and interdependencies between different entities, processes or resources. As a result, the overall presentation of data-flow is characterized by missing facts, processes as well as relations.

During the construction of a KG, synergies will be created and new knowledge will be generated. The main feature of the graph should therefore be that the database that is applied, consists of intelligence features, based on AI-attributes. Based on this intelligence-approach connections between different entities should be created autonomously and logical links should be recognised. Besides, prioritized processes should become visible and restarting times should be noticed at a glance.
In addition, KG should apply the existing knowledge for the creation of new ideas, in a sense to gather new knowledge.

- ➔ **Data correlation has to be visible, therefore an artificial intelligence-based database is required.**
- ➔ **Generation of new knowledge**

A new approach of computing comes to light.

"Big data is high volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization"

(Laney cited from:Janev et al. 2020)

Big Data plays an immense role regarding the implementation of a KG. Huge volumes and high speed of data are considered as the main challenge for today´s operating BCM-systems. As Deutsche Bahn for instance shows, the systems are extremely overloaded due to the huge size of data. A KG is therefore a possible solution to support the BCM-systems by efficiently handling high volumes of data.

➔ **Dealing with Big Data**

Trough the KG synergies should be formed, that generate new insights. This implies that the conduction of tasks or processes twice is avoided.
In this context, also the term transparency plays a relevant role. A system that is transparent, in the sense of the visibility of certain tasks will lead to advantages concerning the working flow due to the higher exchange of information between all participants of the graph.
As a result, the collaboration process between different departments should be optimized, hidden risks become visible and priorities could be better set.

➔ **Creation of synergies**
➔ **Priority setting**
➔ **Transparency**

A further aspect the KG needs to fulfill is the recognition of dependencies, like for example between related processes or resources that are used between more than one department.
Automated recognition between dependencies means that critical processes and their corresponding resources can be easily monitored. In times of crisis or during a break-down the possibility to recognize dependencies means that critical processes and resources could be particularly protected.

➔ **Awareness of dependencies**

6.2. Construction Process of the Inner-Critical-Knowledge-Graph

In consideration of the most significant characteristics that a KG which is applied to the BCM-systems of critical infrastructure organisations has to meet, the construction process of a holistic KG template will be conducted.

The research question that this research attempts to answer is how a template of an innovative holistic KG that could be implemented to the BCM-systems of critical infrastructure organisations looks like.

Within the scope of the present thesis holistic KG-construction-methods were researched that could be applied to the BCM-systems of critical infrastructure organisations. Literature shows that there are various KG-construction-tools, like for instance Knowledge Graph Induction (KGI) by IBM[8]. However, it has been found that KG are mainly applied to single organisations. Furthermore, no literature has been identified that shows a KG application to more than one BCM-system of critical infrastructure organisation. Hence, a research gap has been determined.

For tackling the research question the approach was to build a holistic KG for DB, Austrian Red Cross and DPMA that expands the BCM-systems that are currently in-use. The holistic KG represents a template for each of the three organisations that could be applied to their specific systems. In a first step individual KGs for the organisations interviewed were constructed which were subsequently compared to each other. The intention was that the comparison points out interfaces that turn out to be critical for the proper functioning of a KG, since they occur in the form of the same entity in each individual KG. Thus, the critical-interface-entities were gathered and transformed into a KG which could be applied to all BCM-systems of the three organisations interviewed.

The construction process of the individual graphs has been carried out according to the knowledge-base-triple-method based on the approach by Rusu et al. (2007) which was further supported by an implementation of Zhang et al. (2019). Knowledge is represented in the form of triples. This implies that each fact is based on a triple which consists of a subject, a predicate and an object. Furthermore, each triple represents the connection between two nodes within the KG (Rusu et al. 2007).

The following figure summarizes how the triples-procedure is applied by the illustration of a simplified example (Zhang et al. 2019).

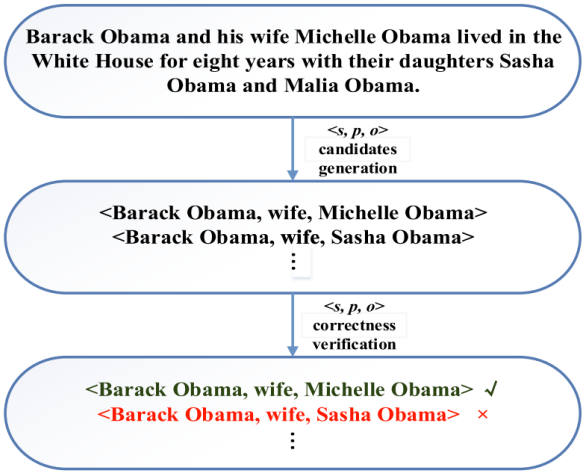


Figure 16: An example of knowledge extraction (Zhang et al. 2019)

[8] https://research.ibm.com/blog/knowledge-graph-ai

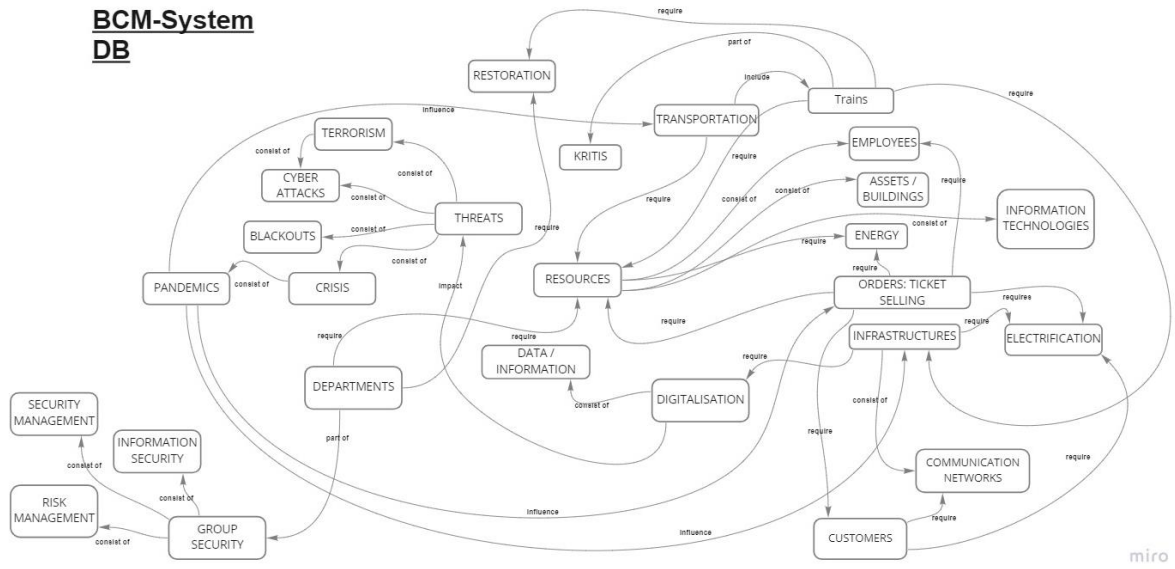
Figure 16 shows an example of knowledge extraction from text. The aim is to create a relation between former US-President Barack Obama and his wife Michelle Obama that could be subsequently implemented to a KG. The procedure illustrates that the first step is the identification process of the subject, predicate and object from text available which is represented as <s, p, o>. After each triple part has been defined the correctness verification follows which is conducted by adding numerical metrics to the triples generated (Zhang et al. 2019).

The triples-procedure has been applied to the data collected during the expert-interviews. Triples have therefore been identified. Due to the fact that a qualitative analysis has been conducted, the correctness verification had to modified because the necessary numerical metrics were missing. Therefore, after the KG-construction process has been finalized, the experts validated the correctness of the triples which were visualized within the holistic KG.

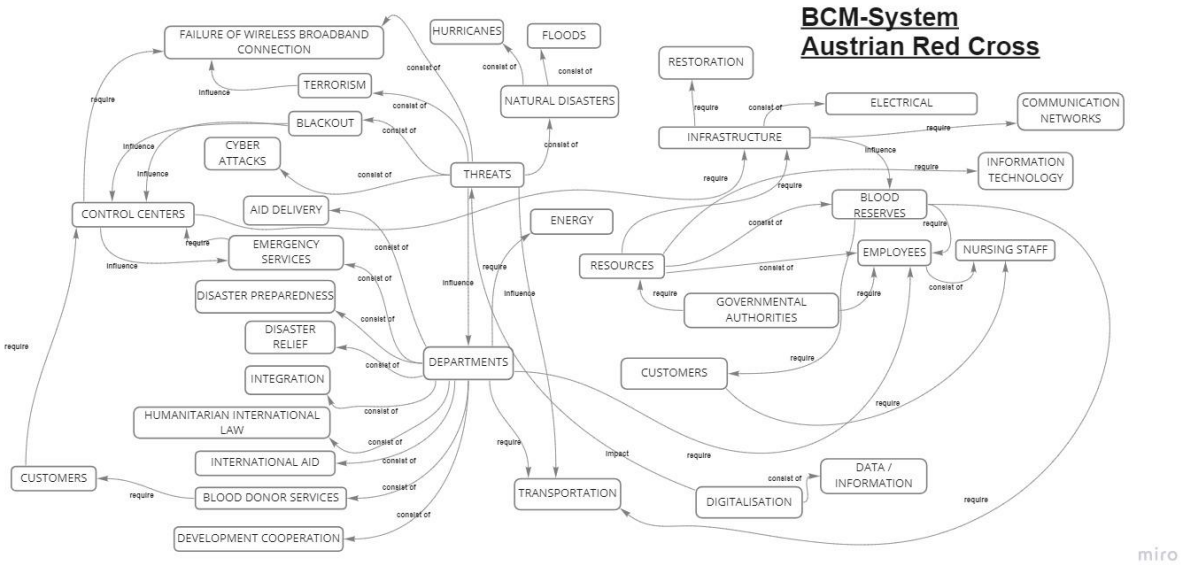
In compliance with the described approach, in the first instance, individual Knowledge Graphs for each critical infrastructure organisation interviewed will be built by applying the knowledge-base-triple-method by Zhang et al. (2019). The single KG are portrayed in the following illustrations.

It should be noted that for a clear and structured representation of a holistic KG that expands the BCM-systems of critical infrastructure organisations only the most relevant entities of the BCM-systems will be covered within the graphs.

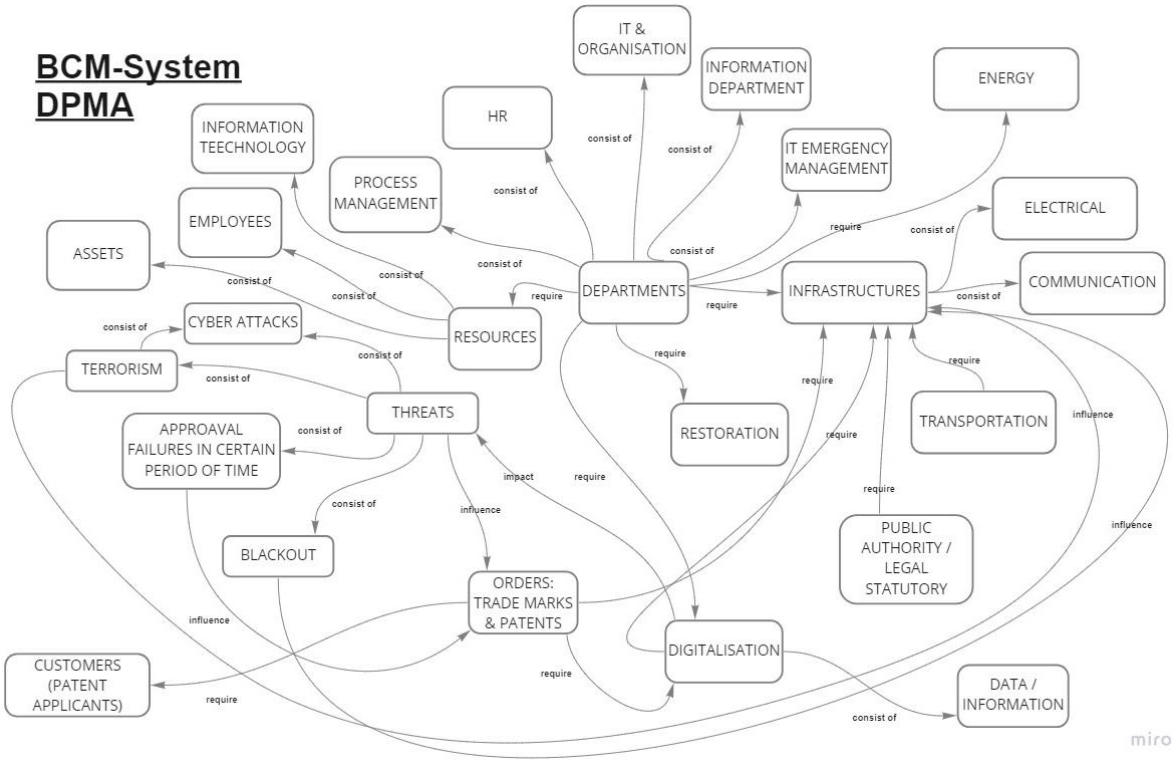
Knowledge Graph Deutsche Bahn



Knowledge Graph Austrian Red Cross

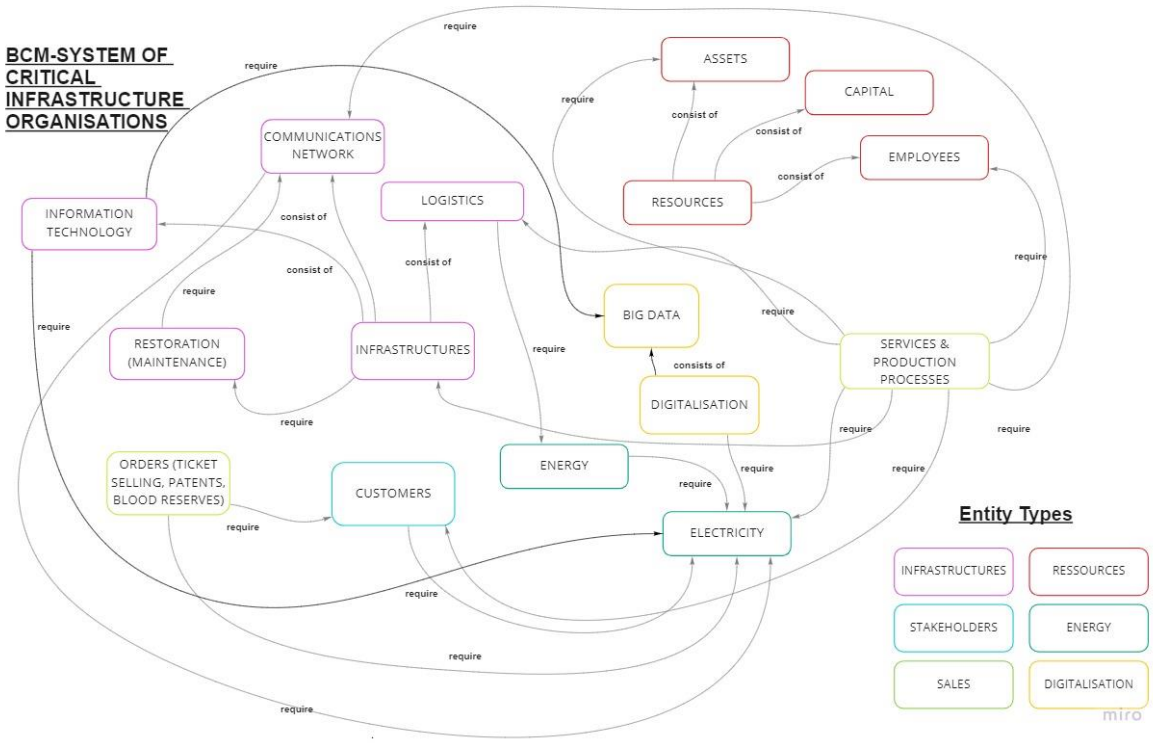


Knowledge Graph German Patent and Trade Mark Office (DPMA)



The Knowledge Graphs illustrate the BCM-systems of DB, Austrian Red Cross and DPMA. All of the relevant entities (subject) and their relations (predicate) to their corresponding nodes (object) are represented based on the method by Zhang et al. (2019).

After each individual graph construction process has been finalised, the question arose which entities a common KG should contain. According to Park et al. (2019) node importance could be estimated using *input importance scores* (Park et al. 2019). This method is based on an exploration of supervised machine learning algorithms. Since data of the individual KGs have been collected by performing a qualitative analysis, the entities of the single KG were compared to each other and their significance was determined according to their frequency of occurrence. All entities which bear a certain similarity were gathered. Subsequently, the common entities were implemented to a holistic KG –the *Inner-Critical-KG*. The name was chosen because it covers all BCM-system-critical entities of critical infrastructure organisations.



By comparing the three individual KG of the critical infrastructure organisations interviewed, it has been observed that the entities of Inner-Critical-KG, were essential to be included in each BCM-system. The Inner-Critical-KG covers most of the system-critical interfaces of the individual KG of DB, Austrian Red Cross and DPMA, however it just represents a template for further applications which implies that not all relevant entities and their relations are visualized. This should also help to ensure that the Inner-Critical-KG is portrayed clearly.

6.2.1. Entities of the Inner-Critical-KG

As the Inner-Critical-KG illustrates many entities of various types, different colors have been selected for a comprehensible representation of each entity types. Those have been divided into: Resources, Energy, Digitalisation, Infrastructures, Stakeholders and Sales.

To contribute to a better understanding of the reader, explanations should be provided how the entity types have been selected. Therefore, the entity type will be further explained within the following paragraphs.

I. Stakeholders

Customers represent one of the main stakeholder groups in all organisations interviewed. At DB customers are passengers that are taking the train, at DPMA patent applicants for instance are counted as customers and at Austrian Red Cross hospitals that require blood reserves are considered part of their clients.

II. Sales

Sales cover all the entities that generate turnover by extension. Therefore, it consists of Orders as well as Services & Production Processes.

Orders are characterized as the entity that further generates revenue for the organisation. For instance, tickets selling, the registrations of trade marks or donations generate business turnover.

Services & Production Processes are the daily business operations and tasks of a critical infrastructure organisation. BCM´s responsibility is to develop process or area specific BC-plans. Therefore, this entity has to be covered within the Inner-Critical-KG.

III. Energy

Electricity

The BCM-system of a critical infrastructure organisation requires energy. In this context, *Electricity* represents the most significant kind of energy as it is a condition for the proper functioning of almost every process and operation that takes place within a BCM-system.

IV. Digitalisation

e.g., *Big Data*

Digitalisation, especially high volumes of data have put new challenges to the BCM-systems of critical infrastructure organisations. Besides, also many new opportunities have emerged due to for instance big data. Therefore, it is considered as a separate entity within the Inner-Critical-KG.

V. Infrastructures

Electrical, Communications Network, Logistics, Information Technology, Restoration (Maintenance)

BCM-systems require infrastructures for their proper functioning. The uttermost important infrastructures for DB, Austrian Red Cross and DPMA could be summarized in the *Electrical, Communications Network, Information Technology, Restoration (Maintenance)* and *Logistics* component. Due to a rapidly changing micro-and macroenvironment of critical infrastructure organisations, regular *maintenance* has a significant role because it is necessary for screening new emerging threats that could impact the BCM-systems. In addition, processes should be maintained and the risk situation should be constantly re-evaluated.

VI. Resources

Assets, Capital, Employees

Resources are summarized in *assets*, *capital*, *employees* and information technology (IT). Those components are essential for all kind of BCM-activities of a critical infrastructure organisation.

The Inner-Critical-KG represents a tool that expands and supports the BCM-systems of critical infrastructure organisations. The following two examples illustrate this more precisely. It is assumed that the trigger for the non-functioning of BCM-systems is always based on internal or external threats. In the following scenarios those hazards are represented in the form of a pandemic and a blackout.

For instance, let's examine the node *Employees* within the Inner-Critical-KG. Let it be supposed that a pandemic hits the world and boarders were closed within the European Union. This real-world scenario actually took place during the first wave of the Covid-19 pandemic 2020. The issue was that foreign workers could not perform their work as they were not allowed to enter the country in which they were

employed. This situation happened for instance to organisations similar to Austrian Red Cross that are operating in the field of 24-hour care as most of their care staff is manpower from abroad. In the case that a KG is implemented to the BCM-system, this scenario could be observed in advance. When picking out the entity E*mployees*, it will become visible how this impacts other entities within the graph. In the present case effects will be remarked in the *Services & Productio*n *Processes* as well as the R*esources* node. Due to the foreign workers that were not available at a certain point of time, resources were not be available. As a result, services could not be completely provided. As a consequence, a part of the system will collapse as too little resources are available.

A further example should contribute to an understanding of functionalities of the developed KG. Under the assumption that a disastrous blackout with power outages hits various European states, the question arises how BCM-systems of critical infrastructure organisations will be affected. The Inner-Critical-KG shows exactly the sequence of entities that will fall out due to power failures. In the present scenario the first entity that fails is *Electricity* because the energy supply cannot be guaranteed anymore. Subsequently, *Services & Production Processes* will be affected as well as *Employees* and other *Resources* that require electricity for their work steps. *Orders*, like for instance ticket selling machines and the approval of a patent cannot be used or carried out anymore. As a further result, the control centres of Austrian Red Cross run out of power which implies that emergency calls cannot be taken anymore. The entire rescue chain will break down due to failures of the *Communications Network* which is relevant for the exchange between the individual rescue units.

A disastrous blackout is considered one of the main threats according to the three critical infrastructure organisations interviewed. Under consideration of the Inner-Critical-KG and the illustration of the domino effect that follows in such blackout-scenario, someone understands why the BCM-division of DB, Austrian Red Cross and DPMA fear such a scenario the most. The blackout affects almost every system-critical entity and could lead to complete system failures.

The first research question was how a template of a holistic Knowledge Graph for critical infrastructure organisation´s BCM-systems look like. The question can be answered with the Inner-Critical-KG that represents a template of a holistic Knowledge Graph for critical infrastructure organisation´s BCM-systems.

The second research question of the thesis regarding the outcomes that can be determined when a holistic KG (the Inner-Critical-KG) is applied to BCM-systems of critical infrastructure organisations has been shown within the two examples above. It becomes visible that the Inner-Critical-KG enables opportunities to generate new knowledge, for instance the identification of the most relevant entities of a BCM-system and the consequences for the scenario that they fail. The gained know-how concerning the node employees could for instance be used for the development of further BC-plans that exactly cover the scenario presented above.

6.3. VALIDATION OF EXPERTS

For testing the hypothesis that the implementation of a holistic Knowledge Graph to the BCM-systems of critical infrastructure organisations improves and expands the systems that are currently in-use at DB, Austrian Red Cross and DPMA a second interview round with the experts was needed for validating the Inner-Critical-KG.

The outcomes of the interviews with DB, Austrian Red Cross and DPMA were based on certain questions that were prepared for the experts in advance. The question covered the following aspects:

- Potentials regarding a better overview of the system, in particular concerning the course of a crisis within the respective organisation
- Potentials concerning the prioritization between single entities

- Potentials regarding benefits after an implementation of the Inner-Critical-KG to the specific organisation

The validations captured during the second-round interviews could be summarized as follows.

The approach of the Inner-Critical-KG to improve BCM-systems has been considered extremely interesting. On the one hand, because the interdependencies in a system are clearly recognisable and, on the other hand, because the course of a crisis within a BCM-system becomes apparent.

The graphical representation contributes greatly to the improvement of the existing BCM-systems. A benefit is therefore seen in an improvement regarding the graphical representation of the BCM-system. Additionally, a benefit is seen in the visualisation of the dense field of activities and performance approach of the organisations. Besides, the issue to see which resources are required for critical processes is considered a further significant improvement.

However, the Inner-Critical-KG could be further developed regarding its semantic distinction of the critical entities. The reason for this is seen in the fact that the Inner-Critical-KG just covers an excerpt of the organisation-specific relevant entities as it constitutes a framework that generally should be used for all critical infrastructure organisations BCM-systems. In this sense, also the recognisability of the temporal or causal sequence in the KG is not particularly comprehensible. In addition, the prioritization between single entities could be improved, as the process is not practicable because the captured entities are considered fundamentally priority entities which implies that it is difficult to objectify a prioritisation.

It would be desirable that the individual entities are presented in a multi-layered way to take into account the complexity of the individual BCM-systems. Furthermore, a distinction regarding the entity energy is suggested as for instance trains at DB require different hertz frequencies as employees within their offices.

To sum up, the Inner-Critical-KG considered a first template for further applications to the individual critical infrastructure organisations represents a tool that the interview-partners could imagine to further implement in their organisations. Especially the visualisation of processes is seen as an improvement of the existing BCM systems. However, during the application process to the specific BCM-systems the focus of further company-specific relevant components in the form of entities has to be carried out. In this sense, it would make sense if the Inner-Critical-KG could be linked to an existing data pool, which is supported by analyses.

In conclusion, this implies that also the hypothesis (holistic KG positively influences the BCM-systems of critical infrastructure organisations) constructed prior to the interviews has been confirmed.

Under the application of the Inner-Critical-KG, BCM receives the opportunity to get insights how a crisis or an incident will pass and which entities will be affected due to a certain crisis scenario. This leads to an improvement regarding the BCM-system. Besides, in the case that one entity fails, further break downs of corresponding nodes will in most cases probably follow. Based on the interconnectedness of the KG it becomes visible in the case that one entity malfunctions what further entities will be subsequently affected.

To sum up, the previous paragraphs show that the overview within BCM-systems of critical infrastructure organisations could be improved by the application of the Inner-Critical-KG. Moreover, it can be quickly recognised what effects the malfunctioning of one unit means for other business areas during an incident or in the case a certain entity breaks down. Additionally, this also offers new possibilities to the BCM-division as they could specifically identify which measures have to be taken at what certain point of time and how priorities should be set.

CHAPTER VII.

Conclusio

The present thesis tackles the significance of Business Continuity Management, especially regarding the emergence of newly crisis. The Covid-19 pandemic represents such kind of crisis. In this context, besides societies and businesses all over the world particularly critical infrastructure organisations were facing major challenges.

It has been observed that the BCM-systems that are currently in-use at Deutsche Bahn, Austrian Red Cross and German Patent and Trade Mark Office are extremely overload due to high volumes and high-speed data. As a result, the effectiveness of the BCM-systems decreases and systems were no longer proper functioning.

For this reason, it has been found that there is a strong need after a further tool that improves the BCM-systems. The Knowledge Graph has therefore been implemented to the BCM-systems of critical infrastructure organisations. The tool aims to expand and support the BCM-systems that are currently in-use.

For the construction process of the Inner-Critical-KG which represents a holistic KG that could be applied by each critical infrastructure organisations interviewed, expectations and needs regarding the characteristics and requirements of such a graph, were gathered during the expert-interviews.

It has been found that the most important features of a holistic KG can be summarized as follows.

- Data has to be evaluated holistically
- Data correlation has to be visible
- Generation of new knowledge
- Dealing with Big Data
- Creation of synergies
- Priority setting
- Transparency
- Awareness of dependencies

Taking into consideration the requirements of the expert-interviews, the Inner-Critical-KG has been subsequently developed. It covers the most critical interfaces in form of entities of the created individual KGs for DB, Austrian Red Cross and DPMA.

In the beginning of the thesis the objective was to identify how a holistic Knowledge Graph for critical infrastructure organisations look like and what outcomes can be determined when a holistic Knowledge Graph is applied to the BCM-systems of the three organisations interviewed.

The corresponding hypothesis stated that the application of a holistic KG supports and expands the BCM-systems that are currently in-use. This proved to be correct. The experts see that a holistic KG implementation can contribute to an improvement of the current BCM-systems. In particular, the visualisation properties of the Inner-Critical-KG are considered a great benefit.

To sum up, the thesis has discovered that the Inner-Critical-KG represents an adequate possibility to expand the present BCM-systems for instance because it could be used as a holistic overview tool that explicitly shows the BCM-corresponding most-critical entities of critical infrastructure organisations. Besides, it is a suitable tool to test scenarios in the event that specific business entities fail. This enables the ability that the BCM-division timely discovers the course of a crisis or the specific impacts that occur due to incidents. These issues have been approved by the experts of DB, Austrian Red Cross and DPMA.

However, it has been further found that the Inner-Critical-KG is just a first template of a holistic graph which implies that there is plenty room for expansion and further applications. Suggestions for further extensions have therefore been gathered during the second-round expert-interviews. However, some features still need to be further developed, like for instance the implementation of an existing data pool to the KG template or the further classification of certain entities, the interview-partners could imagine to implement the Inner-Critical-KG to their corresponding organisations.

In conclusion, it can be stated, that the template of a holistic KG (the Inner-Critical-KG) could be applied by each BCM-system of the critical infrastructure organisations interviewed. However, organisation-specific entities still have to be added. The previous chapters clearly show, how strong the potential of the implementation of the Inner-Critical-KG template to a critical infrastructure organisation´s BCM-system could be. Hence, it is recommended to implement the Inner-Critical-KG to the existing BCM-systems of DB, Austrian Red Cross and DPMA.

List of References

Literaturverzeichnis

Bakar, Zahari Abu; Azbiya Yaacob, Noor ul Sadiqin; Udin, Zulkifli Mohamed (2015a): Business Continuity Management Factors and Organizational Performance: A study on the Moderating Role of it Capability. In: *J Mgt Info* 2 (3), S. 5–12. DOI: 10.31580/jmi.v7i1.38.

Bakar, Zahari Abu; Yaacob, Noorulsadiqin Azbiya; Udin, Zulkifli Mohamed (2015b): THE EFFECT OF BUSINESS CONTINUITY MANAGEMENT FACTORS ON ORGANIZATIONAL PERFORMANCE: A CONCEPTUAL FRAMEWORK. In: *INTERNATIONAL JOURNAL OF ECONOMICS AND FINANCIAL ISSUES* 5.

Bell, Anthony; Quillian, M. Ross (1969): CAPTURING CONCEPTS IN A SEMANTIC NET. Fort Belvoir, VA.

Bellomarini, Luigi; Gottlob, Georg; Pieris, Andreas; Sallinger, Emanuel (2018a): Swift Logic for Big Data and Knowledge Graphs. In: A. Min Tjoa, Ladjel Bellatreche, Stefan Biffl, Jan van Leeuwen und Jiří Wiedermann (Hg.): SOFSEM 2018: theory and practice of computer science. 44th International Conference on Current Trends in Theory and Practice of Computer Science : Krems, Austria, January 29-February 2, 2018 : proceedings, Bd. 10706. Cham: Springer (Advanced research in computing and software science, 10706), S. 3–16.

Bellomarini, Luigi; Sallinger, Emanuel; Gottlob, Georg (2018b): The Vadalog system. In: *Proc. VLDB Endow.* 11 (9), S. 975–987. DOI: 10.14778/3213880.3213888.

Blyth, Michael (Hg.) (2009): Business continuity management. Building an effective incident management plan. ebrary, Inc. Hoboken, NJ: J. Wiley & Sons.

Bordes, Antoine; Gabrilovich, Evgeniy (2014): Constructing and mining web-scale knowledge graphs. In: Sofus Macskassy (Hg.): Proceedings of the 20th ACM SIGKDD international conference on Knowledge discovery and data mining. KDD '14: The 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York New York USA, 24 08 2014 27 08 2014. Association for Computing Machinery-Digital Library; ACM Special Interest Group on Knowledge Discovery in Data; ACM Special Interest Group on Management of Data. New York, NY: ACM (ACM Digital Library), S. 1967.

BRACHMAN, R.; SCHMOLZE, J. (1985): An overview of the KL-ONE Knowledge Representation System. In: *Cognitive Science* 9 (2), S. 171–216. DOI: 10.1016/S0364-0213(85)80014-8.

2020: BSI-Standard 200-4.

Chen, Qiao; Xiao, Hu (2020): A neural knowledge graph evaluator: Combining structural and semantic evidence of knowledge graphs for predicting supportive knowledge in scientific QA. In: *Information Processing & Management* 57 (6).

Codd, E. F. (1970): A relational model of data for large shared data banks. In: *Commun. ACM* 13 (6), S. 377–387. DOI: 10.1145/362384.362685.

Ehrlinger, Lisa; Wöß, Wolfram (2016): Towards a Definition of Knowledge Graphs. In: *SEMANTiCS 2016*.

Fensel, Dieter; Şimşek, Umutcan; Angele, Kevin; Huaman, Elwin; Kärle, Elias; Panasiuk, Oleksandra et al. (2020): Knowledge Graphs. Methodology, Tools and Selected Use Cases. 1st ed. 2020. Cham: Springer International Publishing; Imprint Springer (Springer eBook Collection). Online verfügbar unter http://swbplus.bsz-bw.de/bsz1689100362cov.htm.

Folkers, Andreas (2017): Continuity and catastrophe: business continuity management and the security of financial operations. In: *Economy and Society* 46 (1), S. 103–127. DOI: 10.1080/03085147.2017.1307650.

Gingl, Arno; Buser, Michael (2013): Business Continuity Management (BCM) in Mittelstandsunternehmen (S+S Report 4), S. 50–52. Online verfügbar unter Riskexperts.at.

Gruber, Thomas R. (1993): A translation approach to portable ontology specifications. In: *Knowledge Acquisition* 5 (2), S. 199–220. DOI: 10.1006/KNAC.1993.1008.

Guarino, Nicola; Oberle, Daniel; Staab, Steffen (2009): What Is an Ontology? In: Steffen Staab und Rudi Studer (Hg.): Handbook on ontologies. Second Edition. Berlin, Heidelberg: Springer (International handbooks on information systems), S. 1–17.

Harrington, Brian; Clark, Stephen (2007): ASKNet: Automated Semantic Knowledge Network. Proceedings of the Twenty-Second AAAI Conference on Artificial Intelligence. Vancouver, British Columbia, Canada, 22.07.2007.

Herbane, Brahim (2010): The evolution of business continuity management: A historical review of practices and drivers. In: *Business History* 52 (6), S. 978–1002. DOI: 10.1080/00076791.2010.511185.

Herbane, Brahim; Elliott, Dominic; Swartz, Ethné M. (2004): Business Continuity Management: Time for a Strategic Role? In: *Long Range Planning* 37 (5), S. 386. DOI: 10.1016/j.lrp.2004.07.010.

Hiles, Andrew (Hg.) (2011): The definitive handbook of business continuity management. 3. ed. Hoboken, N.J: Wiley.

Hunziker, Stefan; Meissner, Jens O. (Hg.) (2017): Ganzheitliches Chancen- und Risikomanagement. Interdisziplinäre und praxisnahe Konzepte. Wiesbaden: Springer Fachmedien Wiesbaden.

Janev, Valentina; Graux, Damien; Jabeen, Hajira; Sallinger, Emanuel (Hg.) (2020): Knowledge Graphs and Big Data Processing. 1st ed. 2020. Cham: Springer International Publishing; Imprint Springer (Springer eBook Collection, 12072).

Järveläinen, Jonna (2013): IT incidents and business impacts: Validating a framework for continuity management in information systems. In: *International Journal of Information Management* 33 (3), S. 583–590. DOI: 10.1016/j.ijinfomgt.2013.03.001.

Neches, Robert; Fikes, Richard E.; Finin, Tim; Gruber, Thomas; Patil, Ramesh; Senator, Ted; Swartout, William R. (1991): Enabling Technology for Knowledge Sharing. In: *AI Magazine* 12 (3).

Park, Namyong; Kan, Andrey; Dong, Xin Luna; Zhao, Tong; Faloutsos, Christos (2019): Estimating Node Importance in Knowledge Graphs Using Graph Neural Networks, S. 596–606. DOI: 10.1145/3292500.3330855.

Paulheim, Heiko (2016): Knowledge graph refinement: A survey of approaches and evaluation methods. In: *SW* 8 (3), S. 489–508. DOI: 10.3233/SW-160218.

Pujara, Jay; Miao, Hui; Getoor, Lise; Cohen, William (2013): Knowledge Graph Identification. In: David Hutchison, Takeo Kanade, Josef Kittler, Jon M. Kleinberg, Friedemann Mattern, John C. Mitchell et al. (Hg.): Advanced Information Systems Engineering, Bd. 7908. Berlin, Heidelberg: Springer Berlin Heidelberg (Lecture Notes in Computer Science), S. 542–557.

Qiao, Chen; Hu, Xiao (2020): A neural knowledge graph evaluator: Combining structural and semantic evidence of knowledge graphs for predicting supportive knowledge in scientific QA. In: *Information Processing & Management* 57 (6), S. 102309. DOI: 10.1016/j.ipm.2020.102309.

Rusu, Delia; Dali, Lorand; Fortuna, Blaz; Grobelnik, Marko; Mladenic, Dunja (2007): Triplet extraction from sentences.

Saurugg, Herbert; Pichlmayr, Joe (2013): „Smart“, Vernetzung und Komplexität – Ein Plädoyer für einen kritischeren Umgang mit dem Thema Vernetzung. In: *Elektrotech. Inftech.* 130 (4-5), S. 103–108. DOI: 10.1007/s00502-013-0139-z.

Schepers, Jelle; Vandekerkhof, Pieter; Dillen, Yannick (2021): The Impact of the COVID-19 Crisis on Growth-Oriented SMEs: Building Entrepreneurial Resilience. In: *Sustainability* 13 (16), S. 9296. DOI: 10.3390/su13169296.

Sheth, Amit; Padhee, Swati; Gyrard, Amelie (2019): Knowledge Graphs and Knowledge Networks: The Story in Brief. In: *IEEE Internet Comput.* 23 (4), S. 67–75. DOI: 10.1109/MIC.2019.2928449.

Simmank, Jakob (2020): Eine solche Pandemie gab es noch nie. In: *Zeit Online* 2020, 25.03.2020. Online verfügbar unter https://www.zeit.de/wissen/gesundheit/2020-03/sars-cov-2-pandemien-geschichte-spanische-grippe?utm_referrer=https%3A%2F%2Fwww.google.com%2F.

Speight, Peter (2011): Business Continuity. In: *Journal of Applied Security Research* 6 (4), S. 529–554. DOI: 10.1080/19361610.2011.604021.

Spörrer, Stefan (2014): Business Continuity Management. ISO 22301 und weitere Normen im Rahmen der Informationstechnologie. Wiesbaden: Springer Fachmedien Wiesbaden (Springer eBook Collection).

Staab, Steffen; Studer, Rudi (Hg.) (2004): Handbook on Ontologies. Berlin, Heidelberg: Springer (Springer eBook Collection).

Swarm intelligence for resource management in internet of things (2020). London: Academic Press (Intelligent data-centric systems).

Swartz, Ethne; Elliott, Dominic; Herbane, Brahim; Swartz, Ethné (2010): Business Continuity Management // Business continuity management. A Crisis Management Approach // A crisis management approach. 2nd ed. New York, NY: Routledge.

Swissbanking (Hg.) (2013): Empfehlungen für das Business Continuity Management (BCM).

Unknown (2021): Rotes Kreuz beriet Regierung um 100.000 Euro monatlich. In: *Die Presse* 2021, 03.03.2021. Online verfügbar unter https://www.diepresse.com/5945506/rotes-kreuz-beriet-regierung-um-100000-euro-monatlich.

Uyar, Ahmet; Aliyu, Farouk Musa (2015): Evaluating search features of Google Knowledge Graph and Bing Satori. In: *Online Information Review* 39 (2), S. 197–213. DOI: 10.1108/OIR-10-2014-0257.

Wang, Quan; Mao, Zhendong; Wang, Bin; Guo, Li (2017): Knowledge Graph Embedding: A Survey of Approaches and Applications. In: *IEEE Trans. Knowl. Data Eng.* 29 (12), S. 2724–2743. DOI: 10.1109/TKDE.2017.2754499.

Wei, Li; Le, Xia; Ying, Huang (2020): An Adaptive Ant Colony optimization in Knowledge Graphs. 2020 IEEE International Conference on Knowledge Graph (ICKG). IEEE. IEEE. Nanjing, China, 09.08.2020.

Wille, Rudolf (2006): Methods of Conceptual Knowledge Processing. In: David Hutchison, Takeo Kanade, Josef Kittler, Jon M. Kleinberg, Friedemann Mattern, John C. Mitchell et al. (Hg.): Formal Concept Analysis, Bd. 3874. Berlin, Heidelberg: Springer Berlin Heidelberg (Lecture Notes in Computer Science), S. 1–29.

Wong, Wei Ning Zechariah (2014): Business Continuity Management System. A Complete Guide to Implementing ISO 22301. London: Kogan Page. Online verfügbar unter http://gbv.eblib.com/patron/FullRecord.aspx?p=1825987.

Zhang, Zhao; Zhuang, Fuzhen; Li, Xuebing; Niu, Zheng-Yu; He, Jia; He, Qing; Xiong, Hui (2019): Knowledge triple mining via multi-task learning. In: *Information Systems* 80, S. 64–75. DOI: 10.1016/j.is.2018.09.003.

https://www.dbai.tuwien.ac.at/proj/dlv/tutorial/ (03.08.2021)
https://www.ibm.com/watson (11.08.2021)
https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12462-Protecting-critical-infrastructure-in-the-EU-new-rules_en (08.04.2021)
https://research.ibm.com/blog/knowledge-graph-ai (08.10.2021)
https://www.rki.de/SharedDocs/FAQ/Pandemie/FAQ18.html (01.10.2021)

List of References Expert Interview I: Deutsche Bahn

Saurugg, H., Pichlmayr, J. (2013) „Smart“, Vernetzung und Komplexität – Ein Plädoyer für einen kritischeren Umgang mit dem Thema Vernetzung. Springer Verlag Wien Juni & Juli 2013

Willisegger, Jonas (2018): Schutz kritischer Infrastrukturen. In: Stefan Hunziker und Jens O. Meissner (Hg.): Ganzheitliches Chancen- und Risikomanagement. Wiesbaden: Springer Fachmedien Wiesbaden, S. 61–88.

https://www.bundeskanzleramt.gv.at/themen/sicherheitspolitik/schutz-kritischer-infrastrukturen.html (05.09.2021)

https://www.deutschebahn.com/en/facts_figures-6067278 (22.07.2021)

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12462-Protecting-critical-infrastructure-in-the-EU-new-rules_en (12.08.2021)

Unknown, 13.05.2021 Weltweite Cyberattacke trifft Computer der Deutschen Bahn. Frankfurter Allgemeine. https://www.faz.net/aktuell/wirtschaft/unternehmen/hacker-angriff-weltweite-cyberattacke-trifft-computer-der-deutschen-bahn-15013583.html

List of References Expert Interview II: DPMA

https://www.dpma.de/dpma/wir_ueber_uns/index.html (24.06.2021)

List of References Expert Interview III: Austrian Red Cross

https://www.roteskreuz.at/home (12.05.2021)

https://www.roteskreuz.at/jahresbericht (13.07.2021)

List of Figures

Annex I.

Abstract
The issue of Business Continuity Management (BCM) is highly important, especially regarding the emergence of new crisis. BCM is a method, that is indispensable in various areas. Especially, when it comes to key industries, like critical infrastructures, BCM constitutes an essential part of the operational processes of a company.
Therefore, the thesis deals with the issue of BCM on the one side and the subject of crisis on the other side (inter alia it puts a specific focus on the pandemic Covid-19). Different BCM-systems of critical infrastructure organisations in Germany (Deutsche Bahn, German Patent and Trade Mark Office) and Austria (Austrian Red Cross) will be presented by conducting a qualitative analysis in the form of expert-interviews. Afterwards the results of the interviews will be analysed and subsequently compared to each other.
It has been observed that the existing BCM-systems are extremely overload due to high volumes and high-speed data. As a result, the effectiveness of the BCM-systems decreases, processes got slow and inefficient. To sum up, BCM-systems are no longer proper functioning.
To this end, a further tool that expands and supports the present BCM-systems is required. In the present thesis an application of the Knowledge Graph to the BCM-systems of critical infrastructure organisations is proposed. The developed Inner-Critical-Knowledge-Graph which represents a first approach of a holistic KG-template is illustrated. Its application aims to expand the BCM-systems that are currently in-use by extracting entities and their corresponding relations from data that has been collected during the expert-interviews. The thesis concludes with a demonstration of the outcomes concerning the implementation of a Knowledge Graph to the BCM-systems of Deutsche Bahn, Austrian Red Cross and German Patent and Trade Mark Office.

Abstrakt
Business Continuity Management (BCM) ist von großer Bedeutung, insbesondere im Hinblick auf das Auftreten neuer Krisen. BCM ist eine Methode, die in verschiedenen Bereichen unverzichtbar ist. Insbesondere in Schlüsselindustrien, wie z.B. kritischen Infrastrukturen, ist BCM ein wesentlicher Bestandteil der betrieblichen Abläufe eines Unternehmens.
Die Thesis befasst sich daher zum einen mit BCM und zum anderen mit Krisen (u.a. wird ein besonderer Fokus auf die Pandemie Covid-19 gelegt). Basierend auf einer qualitativen Analyse in Form von ExpertInnen-Interviews werden verschiedene BCM-Systeme kritischer Infrastrukturorganisationen in Deutschland (Deutsche Bahn, Deutsches Patent- und Markenamt) und Österreich (Österreichisches Rotes Kreuz) vorgestellt. Anschließend werden die Ergebnisse der Interviews ausgewertet und miteinander verglichen.
Es wurde festgestellt, dass die bestehenden BCM-Systeme aufgrund der hohen Datenmengen und -geschwindigkeiten extrem überlastet sind. In der Folge sinkt die Effektivität der BCM-Systeme und die Prozesse werden langsam und ineffizient. Zusammenfassend kann festgehalten werden, dass die BCM-Systeme nicht mehr einwandfrei funktionieren.
Aus diesem Grund, wird ein weiteres Tool benötigt, dass die aktuellen BCM-Systeme erweitert und unterstützt. Aus diesem Anlass wird ein Wissensgraph (Knowledge Graph) der Thesis hinzugefügt, der die BCM-Systeme von kritischen Infrastruktur Organisationen erweitern und verbessern soll. In diesem Zusammenhang wird der entwickelte Inner-Critical-Knowledge-Graph vorgestellt, der einen ersten Ansatz eines ganzheitlichen KG-Templates darstellt. Seine Anwendung zielt darauf ab, die BCM-Systeme zu erweitern, indem Entitäten und ihre entsprechenden Beziehungen aus den Daten extrahiert werden, die während der ExpertInnen-Interviews gesammelt wurden.
Abschließend werden die Ergebnisse der Inner-Critical-Knowledge-Graph Implementierung in die BCM-Systeme dargestellt.