

A PRACTICAL APPROACH TO ASSESSING CRITICAL
CONTINUITY PROPERTIES OF ASSETS IN BUSINESS &
IT CONTINUITY MANAGEMENT

PHILIPP CLASSEN

February 2022
University of Twente

Philipp Claßen: *A practical approach to assessing critical continuity properties of assets in Business & IT Continuity Management*, Master Thesis, University of Twente, February 2022

GRADUATION COMMITTEE:

Dr. Ir. Marten van Sinderen

Faculty: Electrical Engineering, Mathematics and Computer Science
Department: Services and Cyber-Security
Email: m.j.vansinderen@utwente.nl

Dr. Adina Aldea

Faculty: Behavioural, Management and Social Sciences
Department: Industrial Engineering and Business Information Systems
Email: a.i.aldea@utwente.nl

Ir. Marcel Brummelaar

Company: Thales Netherlands
Department: IS/IT
Position: IS/IT Projectportfolio Manager & Deputy CPO 9.6 NL
Email: marcel.brummelaar@nl.thalesgroup.com

Ing. Marcel Kerkhof

Company: Thales Netherlands
Department: IS/IT
Position: CISO
Email: marcel.kerkhof@nl.thalesgroup.com

ABSTRACT

In modern days, companies rely heavily on IT systems to support their business. The importance of and dependency on these systems makes it crucial for organisations to operate effectively without unreasonable interruptions. However, it is impossible to mitigate all disasters, and it becomes the question of not if it happens but when a disaster will happen.

This requires that the organisation clearly understands the impact of a disruption on their organisation and has continuity plans in place to mitigate the effects as fast as possible.

To support this assessment, this design science study presents a list of assessment criteria to quantify better the impact of disruptions in an organisation, namely: financial impact, operational impact, third-party impact, regulatory impact and reputational impact. Using two demonstrations to illustrate how the method in combination with the criteria can be applied and what information can be gained. An evaluation with relevant stakeholders indicated that the additional criteria have great potential in quantifying the impact of disruptions and allowing for better investment decisions into continuity management.

CONTENTS

1	INTRODUCTION	1
1.1	Motivation	1
1.2	Thesis Structure	2
2	BACKGROUND	3
2.1	What is Business Continuity Management	3
2.2	BCMS	3
2.3	Business Impact Analysis	4
2.4	Risk Assessment	5
2.5	CIA Triad	5
2.5.1	Confidentiality	6
2.5.2	Integrity	6
2.5.3	Availability	6
2.6	Plan, Do, Check, Act	6
2.6.1	Plan	6
2.6.2	Do	7
2.6.3	Check	7
2.6.4	Act	7
2.6.5	Continuous Improvement	7
3	RESEARCH DESIGN	8
3.1	Research Objective	9
4	LITERATURE REVIEW	11
4.1	Literature review method	11
4.2	Search Steps	11
4.2.1	Collection	11
4.2.2	Cleaning and Selection	12
4.3	Findings	13
4.4	Business Continuity Management Scenarios	13
4.5	Threat and Risk analysis	16
4.6	Criteria	16
4.6.1	RTO & RPO	18
4.6.2	Costs	19
4.6.3	Critical infrastructure	20
4.6.4	CIA Triad	21
4.6.5	Success factors of DRP	22
4.7	Solutions	23
4.7.1	Backup	23
4.7.2	Cloud	24
4.7.3	Hardware deployment	24
4.7.4	Active/Passive	25
4.7.5	Active/Active	25
4.7.6	Active/Active/Passive	25
4.8	Conclusion	26

5	RESEARCH METHOD	27
5.1	Case Studies	27
5.1.1	Analysis of Interviews	27
5.2	Validation	28
5.2.1	Expert Opinions	28
5.2.2	Case Study	29
6	CASE STUDY RESULTS	30
6.1	Summary of interviewed companies	30
6.2	Business Continuity Management practices	31
6.2.1	Standards & Structured approach	32
6.3	Level of Detail	32
6.4	Identified Criticalities	33
6.5	Identified Criteria	34
6.5.1	Financial Impact	34
6.5.2	Operational Impact	34
6.5.3	Regulatory Impact	35
6.5.4	Reputational Impact	35
6.5.5	Third-party Impact	35
6.5.6	Security Impact	36
6.6	Identified Key Performance Indicators	36
6.6.1	RTO	36
6.6.2	RPO	37
6.6.3	MTPD	37
6.7	Pain Points	37
6.7.1	Lack of Integration	38
6.7.2	Insufficient continuity criteria & metrics	38
6.7.3	Lack of requirements	38
6.7.4	Thales specific	38
6.8	Conclusion	39
7	CONTINUITY MANAGEMENT ASSESSMENT METHOD	41
7.1	Continuity Management Stages in a Organization	41
7.1.1	Stage 1: Infrastructure/Application View	42
7.1.2	Stage 2: Process/Value Chain View	42
7.1.3	Stage 3: Continuity by design	43
7.2	Iterative assessment Method	44
7.2.1	Assess	45
7.2.2	Design	51
7.2.3	Implement	54
7.2.4	Validate	56
7.3	Enable the Crisis Management Team	58
8	VALIDATION	59
8.1	IT Security Officer	59
8.1.1	Stages	59
8.1.2	Criteria	60
8.1.3	KPI's	60
8.1.4	Method	60

8.1.5	Scenarios	60
8.2	Continuity Manager	61
8.2.1	Stages	61
8.2.2	Criteria	61
8.2.3	KPI's	62
8.2.4	Method	62
8.2.5	Scenarios	62
8.3	Supply Chain Manager	63
8.3.1	Stages	63
8.3.2	Criteria	63
8.3.3	KPI's	64
8.3.4	Method	64
8.3.5	Scenarios	65
8.4	Chief Information Officer	65
8.4.1	Stages	65
8.4.2	Criteria	65
8.4.3	KPI's	66
8.4.4	Method	66
8.4.5	Scenarios	66
8.5	Summary	67
8.5.1	Usability and Implementation	68
9	DEMONSTRATION	69
9.1	Case selection	69
9.2	PCB Plating machine	69
9.2.1	Process	69
9.2.2	Applied Model	70
9.2.3	Key performance Indicators	72
9.2.4	Impact & Resource Summary	73
9.2.5	Threat Categories	73
9.2.6	Results & Solutions	73
9.3	Conclusion	75
9.4	Remote Access	75
9.4.1	Process	76
9.4.2	Applied Method	77
9.4.3	Key performance Indicators	78
9.4.4	Impact & Resource summary	79
9.4.5	Threat Categories	79
9.4.6	Results & Solutions	80
9.5	Conclusion	81
10	DISCUSSION	82
10.1	Implications	82
10.1.1	Perspective of IT Business Continuity Manage- ment	82
10.1.2	Quantifying the Impact of a disruption	82
10.1.3	The future of IT Business Continuity management	83
10.2	Validity	83

10.2.1	Internal Validity	84
10.2.2	External Validity	84
10.2.3	Construct Validity	84
10.2.4	Reliability	85
10.3	Quality of research	85
11	CONCLUSION	87
11.1	Research questions	87
11.2	Key contributions	88
11.2.1	Contribution to theory	88
11.2.2	Contribution to practice	88
11.2.3	Findings	89
11.3	Related & Future work	90
11.3.1	Limitations	91
I	APPENDIX	92
A	APPENDIX	93
	BIBLIOGRAPHY	97

LIST OF FIGURES

Figure 2.1	PDCA model applied to BCMS processes. From: [23]	7
Figure 3.1	Design cycle adapted from Wieringa	8
Figure 3.2	Design problem template by Wieringa [46]	9
Figure 4.1	Recovery Point Objective (RPO), Recovery Time Objective (RTO), downtime, lost data. From: [29]	19
Figure 4.2	Trade off between cost and time for recovering process. From: [39]	20
Figure 4.3	Conceptual Framework for Factors Influencing The Success of a DRP Process. From [21]	22
Figure 7.1	Stages in BCM	41
Figure 7.2	Method	44
Figure 7.3	Assess assets steps	45
Figure 7.4	BCM key performance indicators	51
Figure 7.5	Design scenario steps	52
Figure 7.6	Implement scenario steps	54
Figure 7.7	Validate scenario steps	56
Figure 9.1	PCB production process - PCBWay [51]	70
Figure 9.2	Simple remote access [50]	76
Figure A.1	Impact Analysis	93
Figure A.2	Key Performance Indicators	93
Figure A.3	BCM key performance indicators	94
Figure A.4	Assess description steps	94
Figure A.5	Emergency Operations Level	95
Figure A.6	Response process	95
Figure A.7	Improve Scenario process	96

LIST OF TABLES

Table 4.1	Found studies and their relevance based on quality criteria (1/2)	14
Table 4.2	Found studies and their relevance based on quality criteria (2/2)	15
Table 4.3	Disaster types	16
Table 4.4	Criteria found in literature	17
Table 4.5	Critical levels to available tiers of recovery strategies	19

Table 4.6	Type of failure costs proposed in American industries. From: [39]	21
Table 4.7	Risk assessment Criteria. From: [4]	22
Table 6.1	Summarized findings of the case studies . . .	39
Table 7.1	List of Criteria with example impact levels . .	48
Table 8.1	Experts interviewed for validation	59
Table 8.2	Summarized findings of the validation interviews	67
Table 9.1	Example assessment of PCB production line .	75
Table 9.2	Example assessment of remote access	81
Table 10.1	Guidelines for design science research by Hevner[1]	86

ACRONYMS

AD	Active Directory
AIM	Access & Identity Management System
BC	Business Continuity
BCM	Business Continuity Management
BCMS	Business Continuity Management System
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BU	Business Unit
CRTO	Cumulative Recovery Time Objective
DRP	Disaster Recovery Plan
ISO	International Organizations for Standards
MBCO	Minimum Business Continuity Objective
MLP	Minimum Level of Performance
MTPD	Maximum Tolerable Time of Disruption
PCB	Printed Circuit Board
RPA	Recovery Point Actual

RPO	Recovery Point Objective
RTA	Recovery Time Actual
RTO	Recovery Time Objective

INTRODUCTION

In the face of a wide variety of crises, ranging from physical disasters such as flooding, loss of power or terrorism to information crises such as internet outages, cyber-attacks and data theft, organisations are investing heavily into mitigating the most severe cases. However, it became apparent that it is impossible to mitigate all disasters, and it then became the question of *when a disaster will happen* and not *if it happens*.

Business Continuity Management (BCM) is the term used when describing the approach an organisation takes to mitigate the impact of a disaster or disruption in one of its assets. While organisations are motivated to limit the impact of disruptions in their organisations, they are struggling with the ever-growing IT infrastructure in the organisation. These highly interconnected and inter-dependent systems are crucial for the organisation's success; however, it becomes more and more challenging to keep on top of the systems, know the complete processes that are performed and remain in control.

1.1 MOTIVATION

In modern days, companies rely heavily on IT systems to support their business. The importance of and dependency on these systems makes it crucial for organisations to operate effectively without unreasonable interruptions. While organisations try to be more or less prepared for catastrophes and natural disasters like flooding, earthquakes and fires, a new threat has risen quickly over the last decade - Cyberattacks.

Not only does it do financial and reputational damage to the organisation, but time and money will also be lost in recovering from such an attack. Depending on the affected IT systems, the whole company might hold if critical IT infrastructure is affected. Companies implement Continuity Management to ensure business continuity and prepare for an unexpected incident that was not mitigated. With the growing threat of cyberattacks, organisations must now prepare for disruptions due to malware, ransomware, and other attacks. Therefore, their continuity management must also include cyberattacks as a potential crisis.

Despite the need for more academic research in this area, organisations are starting to pick up on continuity management on a larger scale and more considerable investments. However, most of the literature is still only concerned with providing general steps for continuity

management and assessing assets. The research aims to provide the first step into more practical assessment while also giving organisations future steps to improve their continuity management systems.

1.2 THESIS STRUCTURE

The following thesis is structured in this way:

- [Chapter 1](#) gives an introduction to Continuity Management and this research
- [Chapter 2](#) gives a background for Business Continuity Management
- [Chapter 3](#) describes the design and steps employed during this research
- [Chapter 4](#) summarised the academic literature review performed for this thesis
- [Chapter 5](#) explains the empirical research methodology followed in this thesis
- [Chapter 6](#) summarised the results of the empirical research
- [Chapter 7](#) introduces the final method
- [Chapter 8](#) summarizes the validation of the draft method
- [Chapter 9](#) shows a sample Demonstration of the process-based assessment at Thales Netherlands
- [Chapter 10](#) discusses the implications of the results for academics and practitioners
- [Chapter 11](#) concludes the thesis

BACKGROUND

This background chapter serves to fill general knowledge about BCM and related topics. This chapter aims at positioning the problem in a clear context.

2.1 WHAT IS BUSINESS CONTINUITY MANAGEMENT

In the face of a wide variety of crises, ranging from physical disasters such as flooding, loss of power, terrorism to information crises such as internet outages, cyber-attacks and data theft, organisations may address each of these crises within their respective business continuity plan. BCM has recently been defined by the International Organizations for Standards (ISO) under ISO-22301:2019 as:

[the] capability of an organisation to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption [24]

BCM originates from the broader area of emergency management, contingency management and disaster recovery planning. The most notable development that led to what we know as BCM was the technological revolution by introducing the IBM 360 in 1965 as a general-purpose business computer and the starting dependency on information systems. In the 1980s, the American government required banks to have a testable backup/recovery plan. Also, the attacks of 11 September 2001 introduced a change in BCM practices, including the concept of organisation-wide resilience with shared ideas about resilience by employees and greater flexibility in the plans developed to respond to large-scale disaster scenarios [19]. At the beginning of the mid-2000s, the internationalisation and standardisation of business continuity management began also partially driven by the introduction of legislation and regulations. Institutes such as the *British Standards Institute* or *International Organization for Standardisation* each introduced their standard at that time, providing a guideline for organisations to implement business continuity.

2.2 BUSINESS CONTINUITY MANAGEMENT SYSTEM

BCM identifies risks and actions taken to treat the risk accordingly to improve the organisation's resilience towards disruptive events. It ensures the development of strategies to maintain the business functions and the needed resources to accomplish those. However, before

this can evolve, the organisation must establish the Business Continuity Management System (BCMS) framework.

Crucial to the success of a BCMS is the total commitment by the organisation's management to the plans and choosing the proper scope and purpose of the plans. Successful strategies and actions can only be developed with a complete understanding of the organisation's context. Therefore, the first task is to understand the organisation's context so that decisions can be made to position the business continuity for success, requiring extensive knowledge of how the organisation is working, including but not limited to culture, products, services, technology, risks and regulations.

The BCMS contains multiple plans that are part of it, detailing specific actions or procedures that should be performed. The Business Continuity Plan (BCP) outlines how the organisation will continue functioning after an unplanned disruption and return to normal business operations at the end. The Disaster Recovery Plan (DRP) is concerned with the full recovery of all affected systems by a disaster and is a subset of the BCP covering *mitigate* and *recover* components.

2.3 BUSINESS IMPACT ANALYSIS

The Business Impact Analysis (BIA) is one of the key activities that have to be performed to develop the BCMS [43]. It is a method used to identify critical business functions or processes in the organisation's context, establish the processes necessary to recover such functions and describe the adverse effects when such a critical function or process is affected for a significant period [9]. According to Sikdar [42], there are three major phases to complete a BIA: data gathering, data analysis and BIA reporting.

2.3.0.1 Data gathering

Data gathering can occur through different means, starting with documentation about the organisation's structure and ways of working, interviews with managers of a department or relevant business units to gain insight into business processes and their dependencies, workshops, video calls or technical documentation and models of overarching infrastructure. Here, the organisation should understand the potential impact of an outage, the maximum time the business can perform without establishing a critical function, legal and contractual implications related to the functions explored, and the financial and organisational impact discussed.

2.3.0.2 Data analysis

Data analysis allows for the structural and logical assessment of the information gathered to facilitate analysis for deciding recovery strate-

gies. A list of all critical business processes has to be made. Again Sikdar [42] identified four criteria on what a critical process is:

- Have a direct, immediate effect in preventing loss of life, personal injury or loss of property.
- Provide vital support to critical functions.
- Mandatory functions (are critical).
- Functions that cannot suffer significant interruption.

These critical processes and their desired levels for an organisation, especially when looking at IS/IT systems, are often linked to the CIA-triad of information security, meaning each function is assigned a *confidentiality*, *integrity* and *availability* level. Furthermore, processes and functions in complex systems of organisations might have interdependencies due to which a noncritical process can become critical due to a critical process depending on it.

2.3.0.3 BIA reporting

The outcome of this, a BIA report, is aimed at heads of departments or other employees in management positions, hence having very little time for detailed explanations. Therefore, only the most crucial information should be present, including critical processes that must be maintained or recovered in case of a disruption, a list of recovery objectives, criteria for ranking, the impact of a specific disruption, recovery strategies and alternatives, and cost-effectiveness solutions.

2.4 RISK ASSESSMENT

Risk assessment, often mixed up with BIA, is used to determine the potential loss of risk in relation to the required costs to mitigate the risk. Although risk assessment is an essential task for BCM, it is not the only source of information for the assessment. A risk assessment identifies threats and vulnerabilities to the organisation's operations, analyses their likelihood of occurrence, and provides control and mitigation strategies [4]. Risk assessment can only cover the known threats to the organisation and will not prepare the organisation for unknown threats.

2.5 CIA TRIAD

CIA is the famous security triangle that provides definitions and criteria which any secure system must meet. These three concepts are also often used in a BIA as criteria for systems and processes. A key concept to understand is that prioritising one or more criteria can

lead to trade-offs in others. This is not necessarily a bad thing, but the choice has to be made consciously [4].

2.5.1 Confidentiality

Confidentiality protects sensitive data and processes from access by unauthorised parties. The data can be exposed for different reasons, such as cyberattacks, data breaches, and unintentional actions by employees. A failure to maintain the confidentiality of information can cause serious harm to the organisation if information such as access codes, product patents, or other valuable information is accessed.

2.5.2 Integrity

Integrity is concerned with the accuracy and completeness of the data. The data should be consistent, accurate and trust-worthy. Ensuring integrity involves protecting data in use, not being changed during transit and at rest and cannot be altered by unauthorised people. Not ensuring or compromising the data integrity means that the data can not be trusted anymore, and an earlier, trusted version of the data has to be recovered.

2.5.3 Availability

Availability is concerned with the accessibility of the system or information for authorised users, ensuring that it can be accessed when needed. It is often associated with reliability or up-time, which can be affected by non-malicious issues like hardware failures or human errors.

2.6 PLAN, DO, CHECK, ACT

The Plan-Do-Check-Act cycle, also known as Deming cycle and mentioned in *ISO 22301:2019*[24] as a management system standard for planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving the effectiveness of an organisation's BCMS. See Figure 2.1.

2.6.1 Plan

In the first step, plan, the organisations establish business continuity policy, objectives, processes, and procedures for their Business Continuity (BC) to align their plan with the organisation's overarching strategy.

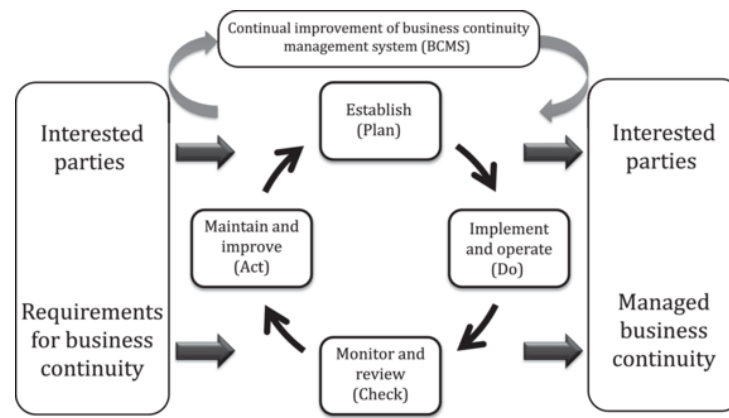


Figure 2.1: PDCA model applied to BCMS processes. From: [23]

2.6.2 Do

Afterwards, the plan must be implemented, and the business continuity policies, controls, and objectives must be operated.

2.6.3 Check

Performance has to be monitored and compared against policies, controls and objectives. Results must be reviewed by management regularly and improvements approved.

2.6.4 Act

Lastly, the BCMS must be maintained and improved over time with corrective actions and the objectives and policies updated.

2.6.5 Continuous Improvement

Often forgotten, and the reason Thales is looking at their BCMS again. IT systems change drastically over time, but the BCP is often not updated, leading to uncertainty over the successful recovery during a disruption. This can be seen on top of Figure 2.1 as the last step to be performed constantly.

RESEARCH DESIGN

This chapter introduces the research design and approach to our thesis in more detail.

This research paper is based on two parts: A descriptive part in the form of a literature review and case studies to answer knowledge questions and a design part for developing an assessment method for continuity management systems. Throughout this thesis, the design science methodology by Wieringa [46] is used. Wieringa provides guidelines for practising information systems and software engineering design science research. According to Wieringa, the goal of a design project is to (re)design an artifact to better contribute to the achievement of a goal.

The design cycle details such a design project which is comprised of three main phases: *problem investigation*, *treatment design* and *treatment validation*. The design cycle is part of a more extensive engineering cycle that incorporates *treatment implementation* and *implementation evaluation* steps.

Depending on the results from the *treatment validation* the cycle might be iterated multiple times over until the designed artefact produced the wanted effect. The design cycle and the question corresponding to each phase are shown in Figure 3.1. Question marks represent knowledge questions, while exclamation marks indicate design problems.

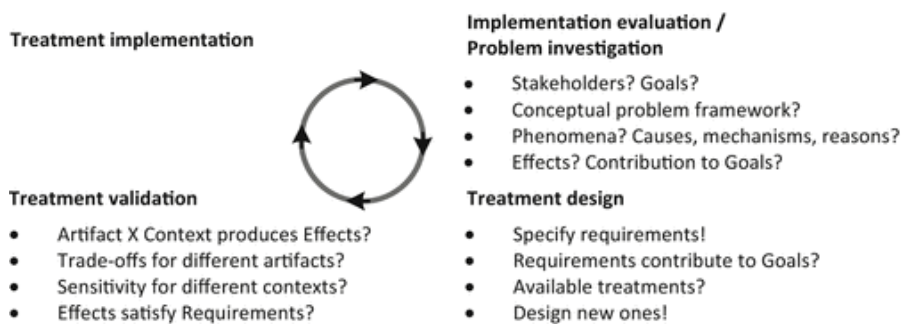


Figure 3.1: Design cycle adapted from Wieringa

3.1 RESEARCH OBJECTIVE

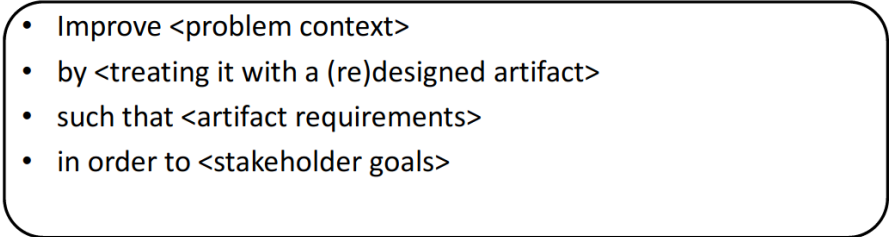
- 
- Improve <problem context>
 - by <treating it with a (re)designed artifact>
 - such that <artifact requirements>
 - in order to <stakeholder goals>

Figure 3.2: Design problem template by Wieringa [46]

Applying the template by Wieringa, the objective of this research can be stated as:

*Improve IT-enabled business operation (in a hostile environment)
by designing a method to assess the critical continuity properties of assets of an organization
that quantifies the impact
in order to ensure business continuity and avoid/minimize impact*

The main research question results from this template and is formulated as:

How can organisations assess their assets in practice in the context of business continuity management?

In order to design an effective method in the problem context, two descriptive knowledge questions must be answered first. Firstly, criteria that organisations are using in practice or are willing to use to assess their assets on continuity have to be identified. Identifying these will aid in designing an appropriate method that provides value to the organisation's assessment. These criteria are expected to vary vastly between organisations and their industry. Therefore, this research aims to identify criteria actively used in continuity management and identify new criteria that organisations would value. The first sub-question is, therefore:

What criteria are used by organizations in practice and which criteria are organizations missing?

The second sub-question aims to identify key performance indicators used to assess the performance or establish requirements for continuity management. Not only should impact be measured for appropriate assessment, but also the performance of continuity solutions should be tracked to understand if improvements are necessary. Therefore, the second sub-question is:

Which key performance indicators are used by organizations in practice and how?

Lastly, an applicable method to apply these criteria and KPI's in practice has to be designed based on the knowledge questions above and must fit into the organisational context of applying continuity management.

Which method should be used by organisations in order to properly assess assets qualitatively and quantitatively while being usable in practice.

LITERATURE REVIEW

The following chapter describes the data collection, filtering and selection for the relevant papers of the literature study and shows the findings and results.

4.1 LITERATURE REVIEW METHOD

This Literature review has been conducted based on the guidelines proposed by Kitchenham, Brereton, Budgen, *et al.* [28] combined with another publication from Kitchenham [8]. Kitchenham identified three essential steps that constitute a systematic review of the literature to provide a balanced and objective summary.

1. convert the need for information (about a technique, procedure, etc.) into an answerable question;
2. find the best evidence with which to answer the question;
3. critically appraise the evidence for its validity (closeness to the truth), impact (size of the effect), and applicability (usefulness);

Next to the literature found by this review, documents from the industry and international standards are considered when discussing the papers. Finally, related industry standards, frameworks, and documents not covered by academic literature are considered.

4.2 SEARCH STEPS

First, a manual search is performed on the digital databases to investigate the wider area and understand the topic. A search query is developed to collect literature documents based on experimenting with different search terms. Several inclusion and exclusion criteria are chosen for cleaning and selecting documents.

4.2.1 Collection

A general search query is created based on the research questions' main concepts and closely related concepts. A search query is constructed to collect studies that discuss business continuity management in IS/IT and their related scenarios and criteria. Closely related to continuity management are availability, recovery, business continuity, and business impact concepts. Also closely related to it are risk analysis, RTO, RPO and DRP.

Scopus: TITLE-ABS-KEY(((("continuity management" OR "availability" OR "recovery" OR "business continuity" OR "business impact" OR "continuity plan" OR resilienc?) AND ("information system" OR "information technology") AND ("risk analysis" OR RTO OR RPO OR DRP)))

Web Of Science: TOPIC: ((("continuity management" OR "availability" OR "recovery" OR "business continuity" OR "business impact" OR "continuity plan" OR resilienc?) AND ("information system" OR "information technology") AND ("risk analysis" OR RTO OR RPO OR DRP))

IEEE: (("All Metadata": "continuity management" OR "All Metadata": "availability" OR "All Metadata": "recovery" OR "All Metadata": "business continuity" OR "All Metadata": "business impact" OR "All Metadata": "continuity plan" OR "All Metadata": "resilienc?) AND ("All Metadata": "information system" OR "All Metadata": "information technology") AND ("All Metadata": "risk analysis" OR "All Metadata": RTO OR "All Metadata": RPO OR "All Metadata": DRP))

4.2.2 Cleaning and Selection

Firstly, a language filter is applied to the found documents, including only documents that have English or no language assigned to them. This inclusion criterion removes six documents, remaining 377.

As this study aims at primary studies, the second inclusion criteria filter on *Reference Type* and *Type of Work*. Only documents with reference type: "Conference Proceedings" or "Journal Article" and type of work: "Article" or "Conference Paper". Moreover, all documents being of type "Review", "Conference Review", or "redacted" are excluded as well, removing 52 - 325 leftover.

As many irrelevant studies related to geographical, coastal and power disaster recovery remain, documents containing keywords *water*, *geographic*, *disease*, *coastal* and *power* are filtered out removing 81 documents, 244 documents remain. Finally, all 20 duplicate records are excluded, leaving 224 left at the end.

Abstract and title for these 224 papers were read, and a first assessment was made on relevance to the topic. Some more missed duplications were identified. Only documents that fulfilled at least the *Open access* criteria and one of the following were considered:

- CR1: The study presents models or frameworks for Business continuity management.
- CR2: The study presents assessment criteria/indicators around business continuity management systems and/or related impact & risk assessment methods.

- *CR₃*: The study presents business continuity or cyber-security scenarios & risks.
- *CR₄*: The study presents solutions that are applicable for recovery plans in business continuity.

These quality criteria reduced the number to 69 papers, removing 155 papers that are not related to the overarching topic of BCM. Of those 69 papers, 41 were not accessible via *Open Access* or the university, leaving 28 papers.

4.3 FINDINGS

This chapter contains the findings of the literature review that has been conducted. The chapter will look at the literature about BCM discuss scenarios and the connected security concerns, as well as discuss the assessment criteria identified in the literature for BCMS solutions.

4.4 BUSINESS CONTINUITY MANAGEMENT SCENARIOS

Current BCMS are concerned with a wide variety of scenarios regarding ensuring continuity and being able to recover.

In 2004, Cerullo and Cerullo [10] analysed national surveys to gain insight into BCP as well as internal and external security threats. At this point, already 75% of organisations worldwide have experienced disruptions due to unexpected unavailability. They also separated internal causes for disasters and external causes and highlighted that most organisations underestimate the potential of internal causes. Mohamed [32] provides an overview of different types of disasters that nearly every organisation faces. While Alhazmi and Malaiya [2] and Gupta et al. [18] each provide a list of disaster causes that are faced by organisations over time, and their contribution to disasters faced overall. A significant share of organisations face disasters related to their IS/IT systems, while most of those causes are not malicious intended. However, in 2013, 63% of the organisations faced cyberattacks or malicious employees. Meilani et al. [30] identified and verified a very similar list of 19 potential disaster causes for a DRP at the Andalas University. Torabi et al. [43] identified 21 risks during the research in an enhanced risk assessment framework for service/manufacturing organisations providing an extensive overview of relevant risk that should be covered in BCM

A combined table with all relevant disasters grouped into internal & external causes as well as more subgroups can be found in Table 4.3.

<i>Documents</i>	<i>CR₁</i>	<i>CR₂</i>	<i>CR₃</i>	<i>CR₄</i>
Alhazmi, O. H. and Y. K. Malaiya (2012). Assessing Disaster Recovery Alternatives: On-Site, Colocation or Cloud. 2012 IEEE 23rd International Symposium on Software Reliability Engineering Workshops, IEEE.				X
Alhazmi, O. H. and Y. K. Malaiya (2013). Evaluating disaster recovery plans using the cloud. 2013 Proceedings Annual Reliability and Maintainability Symposium (RAMS), IEEE.		X	X	X
Angraini, et al. (2018). Risk Assessment on Information Asset an academic Application Using ISO 27001. 2018 6th International Conference on Cyber and IT Service Management (CITSM).		X	X	
Araujo, J., et al. (2018). "Decision making in cloud environments: an approach based on multiple-criteria decision analysis and stochastic models." Journal of Cloud Computing 7(1).	X			X
Baginda, Y. P., et al. (2018). Analysis of RTO and RPO of a Service Stored on Amazon Web Service (AWS) and Google Cloud Engine (GCE). 2018 10th International Conference on Information Technology and Electrical Engineering (ICITEE).	X	X		
Cerullo, V. and M. J. Cerullo (2004). "Business Continuity Planning: A Comprehensive Approach." Information Systems Management 21(3): 70-78.	X		X	
Chen, G. (2012). Improvement Model of Business Continuity Management on E-Learning. Advances in Computer Science and Education, Springer Berlin Heidelberg: 1-5.	X			
Davis, A. (2011). "What Is Critical to Your Infrastructure?" Infosecurity 8(5): 18-21.	X		X	
Dimase, D., et al. (2015). "Systems engineering framework for cyber physical security and resilience." Environment Systems and Decisions 35(2): 291-300.	X	X		
Gerber, M. and R. Von Solms (2005). "Management of risk in the information age." Computers & Security 24(1): 16-30.		X		
Gupta, V., et al. (2016). Exploring disaster recovery parameters in an enterprise application, Institute of Electrical and Electronics Engineers Inc.		X	X	
Hoong, L. L. and G. Marthandan (2011). Factors influencing the success of the disaster recovery planning process: A conceptual paper. 2011 International Conference on Research and Innovation in Information Systems, IEEE.		X		
Huanchun, Y. (2009). A Study on the Risk Hierarchical Model and Risk Conduction Based on the Enterprise Complex Information System. 2009 International Forum on Information Technology and Applications.	X		X	
Katsumata, P., et al. (2010). Cybersecurity risk management. 2010 - MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE, IEEE.	X	X		

Table 4.1: Found studies and their relevance based on quality criteria (1/2)

<i>Documents</i>	<i>CR₁</i>	<i>CR₂</i>	<i>CR₃</i>	<i>CR₄</i>
Mathew, A. and C. Mai (2018). Study of Various Data Recovery and Data Back Up Techniques in Cloud Computing & Their Comparison. 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT).		X		X
Meilani, D., et al. (2019). Designing Disaster Recovery Plan of Data System for University, IOP Publishing Ltd.		X	X	
Mendonça, J., et al. (2020). Multiple-criteria Evaluation of Disaster Recovery Strategies Based on Stochastic Models. 2020 16th International Conference on the Design of Reliable Communication Networks DRCN 2020.	X			X
Mounzer, J., et al. (2010). Integrated security risk management for IT-intensive organizations. 2010 Sixth International Conference on Information Assurance and Security, IEEE.		X		
Păunescu, C. and R. Argatu (2020). "CRITICAL FUNCTIONS IN ENSURING EFFECTIVE BUSINESS CONTINUITY MANAGEMENT. EVIDENCE FROM ROMANIAN COMPANIES." Journal of Business Economics and Management 21(2): 497-520.	X			
Peterson, C. A. (2009). Business Continuity Management & guidelines.				X
Podaras, A. (2015). A Non-arbitrary Method for Estimating IT Business Function Recovery Complexity via Software Complexity. Lecture Notes in Business Information Processing, Springer International Publishing: 144-159.		X		
Rabbani, M., et al. (2016). "Developing a two-step fuzzy cost-benefit analysis for strategies to continuity management and disaster recovery." Safety Science 85: 9-22.	X	X		
Rahman Mohamed, H. A. (2014). "A Proposed Model for IT Disaster Recovery Plan." International Journal of Modern Education and Computer Science 6(4): 57-67.	X		X	X
Sahebjamnia, N., et al. (2015). "Integrated business continuity and disaster recovery planning: Towards organizational resilience." European Journal of Operational Research 242(1): 261-273.			X	
Torabi, S. A., et al. (2016). "An enhanced risk assessment framework for business continuity management systems." Safety Science 89: 201-218.	X	X	X	
Torabi, S. A., et al. (2014). "A new framework for business impact analysis in business continuity management (with a case study)." Safety Science 68: 309-323.	X	X	X	
Wiboonrat, M. (2008). An empirical IT contingency planning model for disaster recovery strategy selection. 2008 IEEE International Engineering Management Conference, IEEE.	X	X	X	
Zare, H., et al. (2020). Business Continuity Plan and Risk Assessment Analysis in Case of a Cyber Attack Disaster in Healthcare Organizations. S. Latifi, Springer. 1134: 137-144.	X			

Table 4.2: Found studies and their relevance based on quality criteria (2/2)

Internal	Humans	Human error, Malicious Employee [30, 32, 43]
	Technology	Hardware Failure, Software Failure, Software upgrade [2, 18, 30, 43] Server down, Internal network disconnected [30] Configuration change, Backup failure, Late backup, Data corruption [30, 32, 43]
External	Natural Disaster	Fire, Flood [2, 18, 32, 43] Earthquake, Tornado [2, 32, 43] Epidemics, Pandemics [32, 43]
	Malicious Actors	Cyber-crime, Security breach, Device theft, Piracy [2, 32, 43] Terrorism, War , Civil unrest, threats [2, 32, 43]
	Third Party	Server down [30] Power outage [2, 18, 30, 32, 43] Disconnected ISP [43] Data Loss [18, 30, 32]
	Politics	Legislative Changes [32, 43]

Table 4.3: Disaster types

4.5 THREAT AND RISK ANALYSIS

Information system risks are complex, interdependent and interact with each other. Mastering risk combinations correctly will help companies take the initiative to avoid risks and solve potential problems, making the information system and information technology an important corporate asset [22]. Risk assessment tries to find the problems of the organisation and makes estimates about potential losses of risk [11]. Threat and risk assessment involves two dimensions, which is measured based on the probability that the threat level will realise, and the impact of the risk [4]. Afterwards, it can be decided to tolerate or accept the risk or implement mitigation strategies. The risk and threat assessment and evaluation are experience-based and require high domain knowledge. Even then, risk analysis is often nothing more than guessing [15]. When assessing risk, especially for disaster cases, a cascading of failures must be considered as this can turn a minor problem into a major crisis [33].

4.6 CRITERIA

This section will consist of the criteria found in the literature for BCMS. Twenty-two articles were identified that discussed different criteria for BCMS. Identifying criteria, mentioned in many papers as a process, has to be performed by an organisation as one of the steps in BCM. The purpose of these criteria is to provide a qualitative and quantitative assessment of an organisation's assets to the management to make appropriate decisions to ensure continuity in the organisation. Unfortunately, the criteria found in the literature are often vague or not named at all; this leaves the organisation with much uncertainty on how to assess their organisation qualitatively.

Category	Criteria	Description
Finance	Cost of failure	Cost of not operating at 100%
	Revenue	Loss of revenue due to not operating
	Productivity	Financial loss due to employees not being able to work
	Countermeasure Cost	Cost of recovering from a disaster
	Investment	Cost of solution to recover faster from disaster
Reputation	Customers	How is the customer affected
Operation	RTO	Amount of time a service can be down and recovered to full operation again without resulting in significant harm
	RPO	Time frame when your data was last usable
	Time to implement	Time it takes to implement the solution
	System performance	Performance capabilities of the new system
	System capacity	Capacity a systems has/needs
	Downtime	Time a service is not available
Regulation	Confidentiality	Level of data sensitivity
	Integrity	Level of data accuracy
	Availability	Level of data availability

Table 4.4: Criteria found in literature

Data centres have turned into the most critical infrastructure for almost all organisations. [48] Consequently, recovering data and systems and returning to normal functions as before an incidence is becoming more and more critical. Researchers focused on storage technology [2], IT disaster recovery site selection [48], business process, as critical techniques [38] to recover from an IT incident.

Wiboonrat [45] identified five different criteria for selecting a disaster recovery solution: *Time to implement*, *RTO*, *Investment*, *System performance* and *System capacity*. He also tried to optimise DRPs by splitting into four different critically levels *Crisis*, *Major*, *Significant* and *Insignificant* with seven different Tiers in total. The research results in four key indicators to measure the critical levels for disaster recovery solutions: Finance, Reputation, Operation, and Regulation.

Time to implement

Time to implement describes the time it takes to implement the new solution into the organisation to help ensure continuity.

System performance

System performance describes the new system's performance in the organisational environment; a change to ensure continuity should not negatively impact the infrastructure and services' performance and ensure agreed performance during a disaster.

System capacity

System capacity describes the capacity a system has to be able to handle during a crisis. A wrongly designed system that can not handle

the load during a disaster will not ensure continuity.

Severity levels

Wiboonrat [45] provided 4 different levels of criticality. The research results in four factors: Finance, Reputation, Operation, and Regulation are the key indicators to measure the critical levels for disaster recovery solutions.

A paper by Mendonça et al. [31], when evaluating stochastic methods for multi-criteria BC strategies, used five different criteria for their model, namely *availability*, *downtime*, *Recovery Point Objective (RPO)*, *Recovery Time Objective (RTO)*, and *costs*.

Downtime

Downtime describes the time when a service or application is not in operation, especially as the result of a malfunction.

Alhazmi and Malaiya [2] also identifies *reliability* as a factor for servers. This factor can be generalised for other IT systems; the higher the reliability is, the less often DRP has to be invoked, and causes such as *hardware failure* are less likely to occur.

Rabbani et al. [39] when researching fuzzy cost benefit analysis focused on financial criteria for BCM, identifying *Outsourcing cost*, *Insuring cost*, and *Failure cost*. These are further broken down in the article for more details.

Most other articles [2, 3, 6, 18, 30, 35, 37, 41] only use RTO and RPO as their main criteria when discussing about BCMS.

4.6.1 RTO & RPO

When discussing BCM, RTO & RPO are currently the two key criteria found in literature when designing the continuity and recovery plans in an organisation and creating the baseline for most if not all BCMS. Knowing the RTOs & RPOs for applications and services across the organisations helps to ensure that strategies are correctly aligned with the needs of the organisation. See Figure 4.1.

Recovery Time Objective

RTO describes the amount of time a service can be down and recovered to full operation again without resulting in significant harm to the organisation. Depending on the importance of organisations services, RTO can be expressed in seconds or up to weeks if necessary.

Recovery Point Objective

RPO describes the time frame when your data was last usable, or in

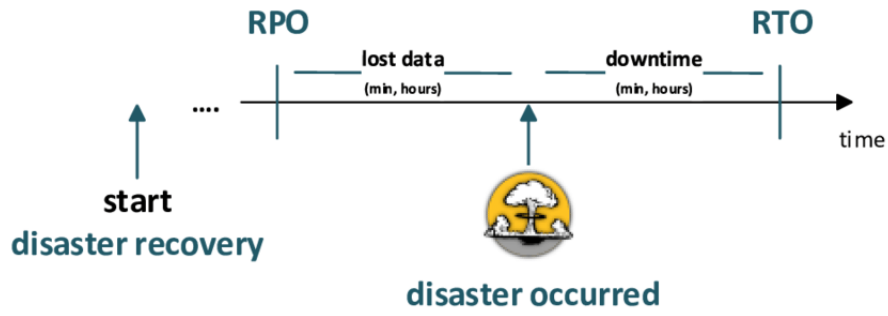


Figure 4.1: Recovery Point Objective (RPO), Recovery Time Objective (RTO), downtime, lost data. From: [29]

Wiboonrat [45]					Podaras [37]	
Critical Level	Tier	Description	RTO	RPO	Tier	RTO
1	1	Point in time backup	2-7 days	2-24hrs	4	< 7 days
1	2	Tape to provisional Backup Site	1-3 days	2-24hrs	3	< 72 hrs
2	3	Disk point in time copy	2-24hrs	2-24hrs		
2,3	4	Remote Logging	12-24hrs	5-30mins	2	< 24 hrs
3	5	Concurrent ReEx	1-12hrs	5-10mins		
4	6	Remote Copy	1-4 hrs	0-5mins	1	< 2 hrs
4	7	Remote copy with Failover	0-60mins	0-5mins		

Table 4.5: Critical levels to available tiers of recovery strategies

other terms, the amount of data that can be lost from a critical event to the most recent backup.

Wiboonrat [45] specified time frames for RTO and RPO for each of his tiers. See Table 4.5 Unfortunately, the tier levels and values are not standard. Alhazmi and Malaiya [2] and Baginda, Affandi, and Pratomo [6] adopted the tiers and values by Wiboonrat, and Mohamed [32] adopted the previous version from SHARE with only six tiers. They can also be defined differently, Meilani et al. [30] established ten levels of severity for the recovery plan of data systems for a university, with five levels for RTO and four levels for RPO. While Podaras [37] used four different levels of impact in his research combined with different values for RTO and RPO. It shows that organisations have different needs; these tiers will likely continue to develop over time when the associated technology advances.

4.6.2 Costs

Costs can be split into two categories from the literature. One is the cost of the solution, and the other is the cost of the failure.

While Cerullo and Cerullo [10] did not highlight criteria related explicitly to BCMS, the indication of costs related to downtime can be seen as one of the relevant criteria. Rabbani et al. [39] shows that it is

essential to ensure the cost-effectiveness of a BCM approach. It helps to give management "a reasonable picture of the costs, benefits and risks associated with a given project so that it could be compared to other investment opportunities". Other investment opportunities could be insuring or outsourcing the risks related to the disasters. Figure 4.2 shows the cost related to recovering from a disaster based on different numbers of RTO and RPO to find the proper balance between costs and minimum requirements for the organisation.

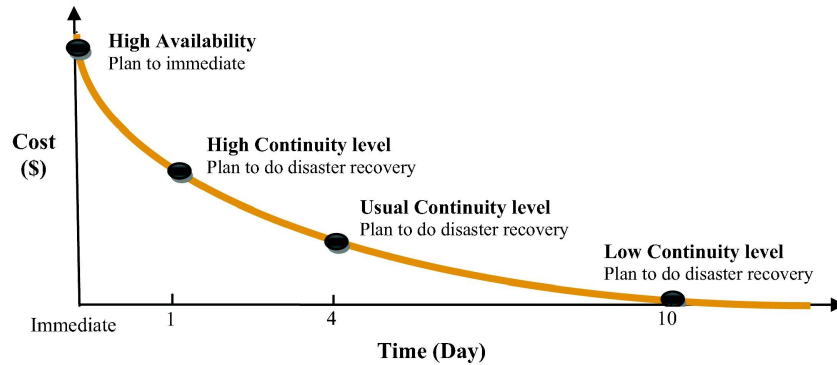


Figure 4.2: Trade off between cost and time for recovering process. From: [39]

Cost of Failure

Cost of failure includes all costs related to the missed level of productivity if the RPO level of the organisation is not 100%. Rabbani et al. [39] identified five categories of failure costs for American industries. See table 4.6.

Alhazmi and Malaiya [2] provides a list of industry-specific revenue loss from 2000, showing that the cost of downtime in the information technology sector was around 1,344,461/hour. Only when the loss of a specific disaster for the organisation is known can a BCMS be adequately designed. Katsumata et al. [26] use the term *countermeasure cost* as implementation costs of a solution to then be able to determinate the cost effectiveness of each countermeasure/solution by evaluating the cost/benefit ratio.

4.6.3 Critical infrastructure

While many articles [6, 10, 11, 13, 14, 18, 21, 30, 32, 35, 37, 38, 41, 43, 45, 48] highlight that the BCMS should first focus on the critical functions of the business or that it should protect critical infrastructure, but most do not provide any information on what a critical function is. Davis [13] provides a statement about a definition for critical infrastructure as:

<i>Failure Cost</i>	<i>Description</i>
Productivity	Number of employees affected, multiplied by hours out, again multiplied by hourly rate
Revenue	Direct loss Compensatory payments Lost future revenue Billing losses Investment losses
Financial performance	Revenue recognition Cash flow Lost discounts (A/P) Payment guarantees Credit rating Stock price
Damaged reputation	Customers, suppliers Financial markets, Banks Business partners
Other expenses	Temporary employees, equipment rental Overtime costs, extra shipping costs Travel expenses, legal obligations

Table 4.6: Type of failure costs proposed in American industries. From: [39]

"Simply put, if the compromise of any part of our organisation's infrastructure would cause a high business impact, it's critical."

Three levels of criticality for infrastructure are used to prioritise, *mission-critical*, *business-critical* and *business operational*. The article also highlights that critical infrastructure is often supported by information systems outside of the organisation's reach and hence outside of the reach of the IT department. Outsourcing and focusing on core competencies can also mean those information systems that support critical infrastructure are not owned by the organisation.

4.6.4 CIA Triad

Angraini et al. [4] uses common risk assessment criteria that are often seen in the BIA and related to the CIA triad. See table 4.7. Mendonça et al. [31] mentioned availability as one of the criteria for BCMS as

<i>Variable of information Security</i>	<i>Assessment Criteria</i>
Confidentiality	1 (public)
	2 (internal use only)
	3 (secret)
Integrity	1 (no impact)
	2 (minor disturbance)
	3 (mayor disturbance)
Availability	1 (low availability)
	2 (medium availability)
	3 (high availability)

Table 4.7: Risk assessment Criteria. From: [4]

well. *Confidentiality*, *Integrity* and *Availability* were used to establish the value of a asset to the organisation in the context of information security.

4.6.5 Success factors of DRP

Hoong and Marthandan [21] bring a completely different view with research about factors influencing success for DRP. The article identifies 12 factors over four domains that influence the success of the disaster recovery planning process, as seen in Figure 4.3.

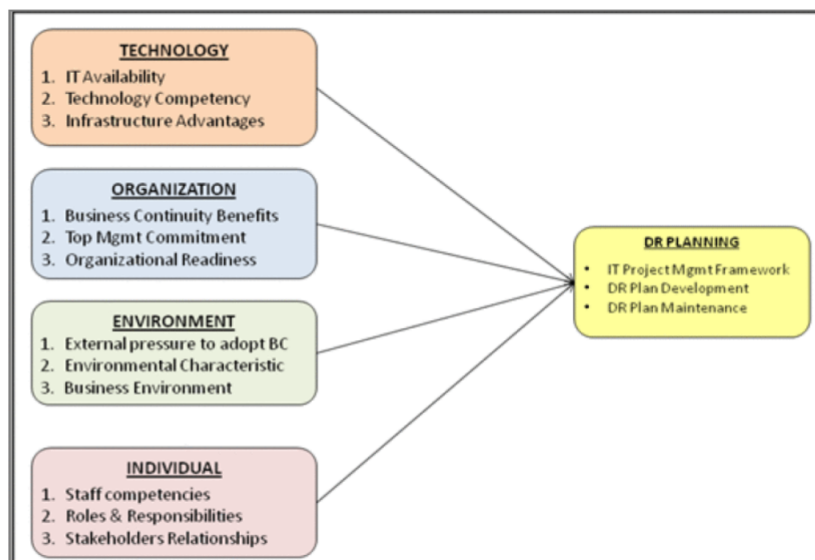


Figure 4.3: Conceptual Framework for Factors Influencing The Success of a DRP Process. From [21]

4.7 SOLUTIONS

This section will provide some solutions for BCMS from the literature and industry documents. These solutions describe general concepts deployed in BCMS to ensure continuity and be prepared for a fast recovery during a disaster. According to Wiboonrat [45] and Araujo et al. [5], the four solutions for disaster recovery strategy are cold sites Tier 1 and Tier 2, warm sites Tier 3 and Tier 4, hot sites Tier 5 and Tier 6, and fault tolerance Tier 7.

Tier 1 & 2 refer to *Cold sites*, being the lowest level of recovery. These are generally rented empty spaces that can be used in case of a disaster, but it could take days to provide viable recovery capabilities with them.

Tier 3 & 4 refer to *Warm sites*. Are slightly above *Cold sites* meaning that there is some equipment is present on the recovery site that can be used in case of a disaster.

Tier 5 & 6 refer to *Hot sites*, one of the ideal solutions for most organisations, where redundant systems and infrastructure try to mirror existing systems, and only data and personnel have to be transferred.

Tier 7 refers to *Fault tolerance*, which is an organisation with a fully parallel IT infrastructure with automatic failover, reducing downtimes to near zero.

4.7.1 Backup

One of the rising approaches to BCM is the adoption of cloud solutions as a feasible backup. Alhazmi and Malaiya [3] discusses 3 different options in the paper: *Onsite*, *Co-location* and *Cloud*.

Onsite: the backup and the system both in one location,

Co-location: the backup site is remotely located.

Cloud: the backup site is located in the cloud

4.7.1.1 3-2-1(-1) backup

In the fields of data backup for recovery, the 3-2-1 rule is often mentioned first. However, the addition of 3-2-1-1 rules for offline backups has been made.

- 3 copies of data
- 2 different media to store backups
- 1 offsite location to store backups online
- 1 offsite location to store backups offline

4.7.2 *Cloud*

However, storing backups in the cloud is not always the best solution for organisations. In an article published later by Alhazmi and Malaiya [2], the concern is that not having complete control over the data can compromise and degrade security due to it being in the cloud. However, researchers have provided evidence that a public cloud might be more secure than a private cloud when the right policies are in place. However, not all organisations can or want to store their most critical data in the cloud.

4.7.2.1 *Disaster Recovery as a Service (DRaaS)*

DRaaS is a cloud service model that organisations can use to back up their data and infrastructure to a third party service. [6] This model means that the organisation does not need to own all resources to handle disaster recovery. Disadvantages are that the organisation gives away control over their disaster recovery. Moreover, no recovery can occur if their DRaaS supplier is affected by the same disaster as the organisation.

Managed DRaaS

Here the third party takes on full responsibility for disaster recovery. This involves closely working with the service provider to keep the infrastructure up to date. This is the best option if the organisation does not have time or resources to manage its disaster recovery.

Assisted DRaaS

Assisted DRaaS uses a third party for disaster recovery, but specific applications might be too complex or sensitive for a third party to take over.

Self-Service DRaaS

With a Self-service DRaaS, organisations are responsible for planning, testing and managing disaster recovery, and a third party only provides backup management software and host backups for the organisation.

4.7.3 *Hardware deployment*

Next to these options, solutions for the recovery sites are often discussed. Different designs in the disaster recovery site allow for better continuity in a disaster.

4.7.3.1 *Symmetric Hardware deployment*

Symmetric hardware deployment describes the setup of identical hardware platforms on both/all data centre sites, allowing for higher availability and performance and the recovery site being sized correctly

and avoiding unexpected problems. However, a fault in the main site can also occur in the recovery site with an identical setup.

4.7.3.2 *Asymmetric Hardware deployment*

Asymmetric hardware deployment describes the setup of different hardware and size for the backup site compared to the main site. This allows the usage of existing equipment, hence being less costly; it also means that a fault related to hardware is less likely to affect both sites. Notably, the disadvantages are that the backup site might not handle the load from the main site during a failover.

4.7.4 *Active/Passive*

An Active/Passive site consists of an active and a passive data centre. The passive data centre is reserved only for disaster recovery in this configuration. If the main active site goes down, the passive recovery site becomes operational[27].

4.7.4.1 *Single Active/Passive*

Single-Active/Passive is the traditional disaster recovery configuration. A single data centre runs all the applications, and a second data centre waits idly until the main site goes down.

4.7.4.2 *Dual Active/Passive*

In the Dual Active/Passive configuration, two sites each have an active component located in the data centre, and a disaster recovery component on-site takes over whenever the main component in the other data centre fails.

4.7.5 *Active/Active*

An Active/Active configuration uses at least two data centres where both can service an application at any time. Each functions as an active application site. Ensuring that applications and services remain accessible if parts of the network or servers fail unexpectedly[27].

4.7.6 *Active/Active/Passive*

An Active/Active/Passive configuration deploys two active data centres similar to an Active/Active setup running all applications and services, but another complete set of application stacks is kept on a third site idling. Whenever one of the active sites fails, the idling backup site can ensure the applications and services continuity[27].

4.8 CONCLUSION

Although the literature has shown that there are different assessment criteria, these criteria are often not operationalised in practice or put into the context of a business continuity assessment. Most papers focus on the general approach to continuity management and provide rough guidelines on which steps should be taken for continuity management and mention some well-known criteria, [RTO](#) & [RPO](#). However, rarely are criteria explicitly mentioned, and methods for a clear approach to assessing the impact in continuity management has been proposed, and no list of operationalised criteria has been made. Although organisations deploy continuity management systems and perform impact assessments in many ways, no empirical research and quantitative data have been encountered during this research showing that certain approaches and criteria are used more often and successful.

This lack of research in continuity management for IS/IT shows there is a need for a practical and general method for assessing and evaluating assets in an organisation and providing an operationalised and quantifiable list of criteria. When the organisation fully understands the impact and damage due to disruption, it develops and deploys successful strategies to mitigate or limit such disruptions.

RESEARCH METHOD

5.1 CASE STUDIES

It is essential to conduct an empirical research practice within this study to deal with the lack of empirical studies within the topic of continuity management to increase the credibility of the conclusions and allow us to base the continuity method in a real-world and practical context. Therefore, we chose a multiple-case approach, following Yin's [47] methodology, along with the replication approach. This places continuity management approaches as the focus of this analysis, and multiple companies are analysed to allow the observations to be compared potentially generalised for a wider group.

Semi-Structured Interviews:

Semi-structured interviews were the main contribution to the case study. At least one interview was conducted in each case study, leading to 11 interviews over nine organisations. Interviewees were selected based on their experience with continuity management and their position in the organisation. Interviews were held either individually or as a session with multiple people via virtual meetings.

Informal Conversations:

Remarks made of the record were taken into account when appropriate and as long as they did not concern any confidential information.

Additional Information:

In some cases, additional information was shown via screen sharing to understand the organisation and their processes better. Again, these were taken into account as long as they did not concern any confidential information.

5.1.1 *Analysis of Interviews*

All interviews were recorded with the permission of the respondents. The recordings were transcribed following the interview sessions to be as complete as possible. Conversation parts that did not directly answer the research questions were omitted. In some cases, names were redacted for anonymity. Afterwards, the transcripts were sent to the interviewees, who were given the opportunity to give feedback

and remarks. Interviews usually lasted 60 minutes; however, some interviews took longer due to engaging discussions.

Following the concept of *open coding*, ATLAS.ti - a qualitative data analysis coding tool was used to analyse each interview. Codes were assigned to sentences or sections of the interview describing the topics discussed there. Beginning with codes related to concepts identified in the literature review, many more codes were added during the coding process to capture as much contextual information as possible. Later, codes were merged when describing similar concepts and grouped into categories when codes were related to similar concepts. Overall, 54 codes were identified in the end.

5.2 VALIDATION

To validate the method proposed in this research, Venable et al. [44] describes two different dimensions for validating design science research, *formative* and *summative* evaluations of the model as the first dimension and *artificial* and *naturalistic* evaluation as the second dimension. While *Formative* evaluation focuses on improving the artifact, *summative* evaluation focuses on placing the artifact in different contexts to gain a better understanding. *Artificial* evaluation uses laboratory experiments, simulations and theoretical arguments while *naturalistic* evaluation tries to examine the artefact in a real-world setting.

Following this approach, this design science research applies the *Technical Risk & Efficacy* evaluation strategy by Venable [44]. This strategy starts with artificial formative evaluation iterative in the beginning and moves towards a more summative artificial method to determine that the utility of the artefact is derived from the use of the artefact and not other factors. Later, the strategy engages in more naturalistic evaluations.

Our research starts the artificial formative evaluation by interviewing multiple experts at different organisations to improve the artefact iteratively. Afterwards, a more naturalistic evaluation was conducted via a small sample implementation on two processes. Later the process owner can give feedback on the usefulness and effectiveness of the method and criteria for a practical impact assessment.

5.2.1 Expert Opinions

To validate the (IT) continuity management method, experts' opinions in continuity management, IT and operations were collected. Following Wieringa's Design Science Methodology [46], this comprises of:

"The design of an artifact is submitted to a panel of experts, who imagine how such an artifact will interact with

problem contexts imagined by them and then predict what effects they think this would have." (Wieringa, 2014, p.63)

None of the experts was involved before this validation step to gather their unbiased views on the approach. The sessions consisted of many discussions about concepts present on slides. In the end, all feedback by the expert was written down in summary. The iterative approach allowed each interviewee to see a more refined version of the method.

5.2.2 *Case Study*

Small sample implementations were performed on two simplified processes inside Thales, with a version of the method created in the last phases of the research. The implementation contained a short explanation of the process, an assessment of the process with the method proposed in this research with relevant criteria, followed by possible response options that the organisation could take.

CASE STUDY RESULTS

The following chapter will first introduce the interviewed organisations, followed by the presentation of results from the case study that will be used in the design of the method in Chapter 7.

6.1 SUMMARY OF INTERVIEWED COMPANIES

The following section will shortly describe the case study companies that participated. Most companies will not be named directly and only mentioned as part of their respective sector due to promised anonymity. All companies mentioned that they had continuity management systems in place with varying approaches; therefore, this chapter's analysis will highlight the differences and similarities of their approaches.

Start-Up:

Start-Up is a small start-up company in the Netherlands providing cloud services to larger organisations. The interviewee is a security officer.

FinTech Company

FinTech is a dutch firm in the financial services industry, which outsourced large parts of their continuity management systems to BCM cloud providers and ensured their capabilities via reviewing their providers. The interviewee is a security officer.

Banks

Bank NL and Bank GER are two large banks located in the Netherlands and Germany. Due to many regulations and requirements, these two banks have implemented continuity management practices for a long time and have established transparent processes and strategies. The interviewees were both BCM managers in the central IT department.

Insurance Company:

Insurance company is a large insurance company located in Germany. In recent years, they have been heavily transitioning their continuity management approach with a very proactive approach. The interviewee is a BCM Coordinator at the central IT working towards the main BCM manager who is setting the specifications for the business guide-

lines in BCM.

Governmental Departments:

Gov. Dept. 1 & 2 are two similar IT departments from the dutch government running highly complex IT infrastructure used by almost all citizens in the Netherlands regularly. The Interviewees were two Continuity Management Advisors for Gov. Dept. 1 and a Security officer for Gov. Dept. 2.

Thales Netherlands:

Thales Netherlands, the organisation for whom this research is conducted. Thales Netherlands is a subsidiary of the French Thales Group. Thales has been implementing continuity management practices for more than ten years but recently started to look into their approach and potential improvements. The interviewees were an Enterprise Architect, BCM Manager and CISO.

Thales Germany:

Thales Germany is the German subsidiary of the French Thales Group. They were chosen for being technically part of the same organisation but to investigate the differences and similarities between the two subsidiaries. The interviewees were two BCM managers, one from the business side and one from the technical side.

6.2 BUSINESS CONTINUITY MANAGEMENT PRACTICES

At the start, the interviewees were asked to describe their understanding of BCM, followed by how BCM was implemented at their organisation. This was used to better understand the implementation at the organisation and their general approach towards BCM. Different levels of sophistication were present between the different organisations, ranging from basic implementation of BCM to advanced BCM strategies encompassing the entire organisation with further transformation. The interview considered different concepts like level of detail, assessment criteria used, organisation coverage, or approach. For example, multiple organisations indicated that their current BCM strategy mainly focuses on the hardware level of the IT like "*recovery of a Datacenter*". Others already take a deep look into all organisational processes and evaluate their organisation based on the value generated by these processes. In contrast to those, others indicated that their BCM strategy is automated and fully outsourced to third parties, giving away control but also responsibilities to another party with *DRaaS*.

This is very important when designing a method for BCM practices, as an organisation might need to take in-between steps towards their intended goal before successfully improving its capabilities.

6.2.1 *Standards & Structured approach*

Of interest was also the approach organisations took for their BCM strategy. From the literature, we have seen that standards and scientific papers often do not provide (a lot of) practical guidelines to the organisations for BCM. This is also found with the respondents' organisations - here; almost all organisations use general concepts found in (grey) literature like using a BIA. However, most admit that their approach is mainly based on their design, supported by the different approaches seen between the organisations. Standards like [ISO](#) or similar are often used to give an idea for an approach but often lack the essential details, like explicit criteria, that would help organisations in implementing continuity management practices.

6.3 LEVEL OF DETAIL

Since the first part of BCM practice is to assess the infrastructure/elements of the organisation, we were interested in which level the organisations look at themselves. These levels describe an organisation's perspective when assessing its enterprise infrastructure.

Firstly, a big part of the organisations agreed that they mainly look at the hardware level of their organisation as they are trying to create a basic level of recovery capabilities. The reasoning here is that before any other capabilities can be established on top of it, the organisation must handle disruptions on a simple hardware level. This is also supported by more progressive organisations who highlighted that they too started with the hardware level before progressively improving on top of it.

Secondly, Thales Netherlands and Gov. Dept. 1 showed that their current view is focused on an application level of the hardware level. The reasoning behind this is based on the underlying hardware. Specific applications and the related data that might be more or less relevant to the organisation could require different hardware. To be more efficient with their resources, not every application might need high-speed storage in the primary and backup site or contains confidential data that needs to be protected by all means. Hence, a separation based on the application level has been done. One of the considerable shortcomings here is that the dependencies are unclear. One application might break due to another application breaking in the first place, but this is not captured in this view.

Next, *Insurance Company* indicated the subsequent step, *Process/-Value Chain level*, that has been done by organizations. The viewpoint shifts away from isolated applications and hardware and focuses on a process/value chain based perspective. Applications do not have an intrinsic value to the organisation unless they are used in some way to generate value. This more advanced practice focuses on processes and all their dependencies connected to them. This perspective allows the organisation to assess better how they are generating value. Processes that generate the most value for the organisation should be protected, and their continuity ensured before others. Taking a process-based view also naturally includes most dependent resources related to a process as they should be included in a process model.

Next, as deployed by FinTech, is the outsourcing of continuity management to third party cloud providers. Especially for smaller organisations, this allows for a good BCM strategy where the organisation has given away the responsibility to a third party. A security review is performed at the provider to ensure that all BCM criteria are met for the organisation. One of the considerable shortcomings here is that the organisation gives control over its BCM strategy away and has minimal capabilities.

Lastly, a concept that all large organisations mention in one way or another from now on is called "*Continuity by Design*" and often highlighted as an idea that the respondents would like to see in the organisation. This is based on the notion that Continuity Management is often seen as an afterthought and not as a core requirement. Infrastructure is designed and implemented, and only afterwards is continuity management considered; changes are made without considering the impact on BCM. This costs extra resources and is counter-productive as IT infrastructure is often very complex, interconnected, and can not easily be changed again.

6.4 IDENTIFIED CRITICALITIES

Criticality was another often mentioned concept for organisations. Every assessed element received a criticality rating to determine the organisation's importance and required recovery speed. The more critical an element is, the faster an organisation wants it back up and running. Multiple respondents used names like *mission-critical*, *critical* and *non-critical* for their ranking. Variations used by some correspondents were *business-critical* which replaced *mission-critical*.

However, almost every organisation admitted that they did not clearly define these "criticality" concepts and the differences. This can be problematic when the organisation prioritises what they want to

ensure continuity, as the set criticalities might not be consistent.

6.5 IDENTIFIED CRITERIA

As one of the main goals following the literature study was to identify the criteria that are used to assess the infrastructure in BCM at an organisation, respondents were asked which criteria they use followed by a discussion about criteria found in the literature and their perceived usefulness for the organisation in assessing the impact. These criteria are also related to common enterprise risks organisations might encounter.

6.5.1 *Financial Impact*

Financial Impact is the criteria found most often in the literature, describing the direct financial loss to the organisation when a disruption occurs, as the financial loss of a machine due to damage or the replacement of a server part due to malfunction. During the interviews, most organisations confirmed that they do not have a clear picture of the financial damage of disruption and that they also do not quantify it. Contrary to that, *Insurance company* and *Start-Up* do make use of financial impact criteria and assess the direct loss of a disruption. To simplify the classification, they make use of financial loss categories like "between €50.000 and €100.000".

For some organisations, the lack of quantifying financial loss was justified due to other criteria being more relevant at the given time. However, organisations agreed to assess the financial impact, especially when compared to an organisation's risk appetite, often expressed in monetary values.

6.5.2 *Operational Impact*

Next, to direct financial impact, there is also the *operational impact*. As continuity management is concerned with recovering services, processes and production in an organisation, every disruption will affect the organisation's operations. Here, organisations had very different approaches to it. Some organisations did not use this criterion as it was not deemed necessary; others used it indirectly when deciding criticality based on active users. Overall, organisations agreed that the operational impact must be assessed as it can be a substantial impact when disruptions affect many users or go on for a long time. Nonetheless, there was no explicit consent on assessing this criterion. Different ideas were provided like measuring the operational costs

that would occur regardless of disruption, and others proposed to focus on the most significant contributors, employees and their salary, e.g. *"more than 1000 employee hours lost per hour downtime"*

6.5.3 *Regulatory Impact*

Regulatory Impact was seen as the biggest concern by organisations in the financial industry like Bank GER and Bank NL. As their sector is highly regulated and they are required by law to ensure continuity of their services and customers are likely to complain quickly, they see the regulatory impact as a core criterion for their assessment. Other organisations like Thales Netherlands indicated that the regulatory impact might be a useful criterion for them as they act in the defence sector and under strict regulatory oversight. However, this criterion is used very sparsely, and most organisations are unsure if it adds enough value to their assessment to warrant the effort to establish it.

6.5.4 *Reputational Impact*

Reputational Impact is seen by most organisations as very important. Gov. Dept. 1 indicated this as their main criteria for continuity for citizen-facing services. Bad reputation at Gov. Dept. 1 would potentially lead to citizens not paying their taxes, violating rules or generally losing trust in the government. Organisations like Thales and Insurance Company also see the reputational impact as an important criterion due to their current vision *"Thales's core purpose is to build a future we can all trust"* that can not be achieved if they have a bad reputation.

6.5.5 *Third-party Impact*

Third-party Impact brought into the discussion by Gov. Dept. 2 and also indicated by two other organisations concerns a qualitative assessment of the involvement of third parties for the assessed element. Whenever a third party is involved, ensuring continuity becomes more difficult due to multiple organisations working together. If, for example, the third-party supplied service is disrupted, organisations relying on that service cannot recover this disruption themselves. Therefore, the organisation must know what it means for them if the third party encounters a disruption and what the organisation can do to mitigate it as much as possible on their side. A recent example of what kind of impact third parties can have and what kind of core functions they fulfil for some organisations is well demon-

strated by the SolarWinds attack. The provided impact levels in Table 7.1 have been designed for this method in collaboration with Thales, trying to generalise for most cases present in Thales.

6.5.6 Security Impact

Lastly, *security impact* was first captioned at Thales Netherlands during the investigative phase. Here an assessment for *Confidentiality*, *Integrity* and *Availability* was performed as part of the BIA. This has not been found at any of the other organisations in a similar fashion. FinTech, Gov. Dept. 1 and Bank NL indicated that they consider security in their BIA; however, the other companies mentioned that this criterion is more often included in the risk analysis for mitigating problems than in continuity management. On the other hand, most organisations also indicated that they could see the added value for continuity assessment, at least when looking at IT.

6.6 IDENTIFIED KEY PERFORMANCE INDICATORS

Next to identifying and assessing continuity management, it is also essential to see how organisations evaluate their strategies. This is required to understand if the chosen strategy and solution can achieve the intended continuity goal as without any measurable success indicators, it becomes challenging to assess the current continuity capabilities and improve over time.

6.6.1 RTO

Recovery Time Objective, describes how quickly a system needs to be recovered after downtime so that there is no significant impact to the organisation. This is a key metric seen in all other scientific literature and extensively used in the industry. Every interviewee indicated that this is one of the key indicators used and established for BCM. It creates the baseline that an organisation tries to achieve; such a baseline can range from "less than 15 minutes" to "more than 1 week", similar to what Wiboonrat [45] proposed in his paper. Every organisation mentioned a similar notion for this KPI used generously throughout the BCM strategy. However, the Insurance Company indicated that too many systems are labelled with too fast recovery times. Reasoning that most systems, even when disrupted, would cost the organisation much money but would not bring the organisation into financial or operational trouble if disrupted for 24 hours instead of 15 minutes. This notion has been brought into later interviews and generally agreed to by others. On the other hand, Thales indicated that they are trying to reduce the recovery times on an application level

to near zero with a redundant active-active infrastructure to achieve a near-instant failover.

6.6.2 RPO

Recovery Point Objective describes the maximum time that data is lost from disruption, a criterion often found in the literature and also used by all organisations in their BCM strategy. Most organisations indicated that they usually consider an RPO of 24 hours, meaning a backup of the data is made every 24 hours so that they maximal lose 24 hours worth of data. Organisations like Bank NL and Bank GER use shorter intervals for systems like banking transactions. Here the business can not afford to lose more than 1 hour of data. This also shows a wide variety of RPO values that should be used inside an organisation to protect the systems with the required resources accordingly.

Multiple organisations consider RPO & RTO as fundamentals and see them as KPIs that have been around for a long time already and might be a bit dated if those are the only ones used.

6.6.3 MTPD

Maximum Tolerable Period of Disruption, the duration after which an organisation's viability will be irreparably damaged if a product or service delivery cannot be resumed. - BCI's GPG [20]

When brought up during the interviews, organisations often directly link it to the RTO, with it being the same or just a higher number. Based on the current definition, organisations are struggling to establish this value in a meaningful way. It is usually complicated to know when the organisation received irreparable damage due to the disruption of a specific service. Multiple other organisations confirmed this notion, and everyone has a slightly different understanding and meaning to this KPI. Hence it becomes apparent that this KPI requires a clear definition used in practice.

6.7 PAIN POINTS

Next to the criteria and key performance indicators, the interviewees brought other concerns, problems, and general pain points. As the planned method attempts to be practically oriented, these pain points were also analysed and used for the design of the method. Some are

overarching problems that are partially covered by the criteria and KPI's while others are of a more strategic and organisational nature.

6.7.1 *Lack of Integration*

lack of integration, many of the larger organisations, including Thales, mentioned during interviews that continuity management is not yet very integrated into the organisation - often described as "an afterthought" or "a budget issue". This is a problem when the Continuity management team has to ensure continuity on already implemented systems and when they have to communicate with other teams in the organisation. Even inside the IT departments, very few employees outside the BCM teams know what BCM is and why it is important. However, we see BCM on a similar level to security, and it should also be a core part of an organisational approach. Some interviewees also highlighted that they are considered "continuity advisors" and not "continuity managers" and only provide advice on what should be done but are not in the position to make the final decisions.

6.7.2 *Insufficient continuity criteria & metrics*

As seen in the criteria and metrics section above, most organisations only use a tiny subset of the overall criteria and could gain a lot more insight into their infrastructure and capabilities using more quantifiable criteria. Moreover, the lack of KPI's used at organisations makes it difficult to gain a clear overview of the intended and actual capabilities of the continuity team and their approach.

6.7.3 *Lack of requirements*

Lastly, the organisations' lack of continuity requirements supports the notion of "an afterthought". Newly developed projects still do not have continuity requirements from the beginning and are often finished and put into production before testing the continuity capabilities. This leads to a catch-up game for the continuity team and puts the organisation at risk. This also includes the lack of general continuity requirements like yearly reviews.

6.7.4 *Thales specific*

As this research is done at Thales Netherlands, more insight was collected there, and some more pain points were identified that could be generalised for other organisations in a similar position.

6.7.4.1 No infrastructure mapping

The larger the (IT) infrastructure gets, the more complex and inter-dependent the systems turn out. Often these systems are so large that it becomes tough to have and keep a clear overview of dependencies and connections inside the infrastructure. Not only is a clear overview of the dependencies crucial for the proper assessment, but it also helps with keeping up to date in a continuously changing (IT) infrastructure.

6.7.4.2 No unified approach

As the last point, Thales group and their subsidiaries do not have a unified approach toward continuity management. In consequence, each subsidiary developed its approach toward continuity management. This makes it challenging to learn from each other's actions, compare their performance or even help each other during an emergency.

6.8 CONCLUSION

Category	Findings
Level of details	Hardware view, application view, process view
Criticalities	Mission-critical, critical, non-critical
Criteria	Financial, operational, regulatory, reputational, third-party, security
Key performance indicators	RTO, RPO, MTPD
Pain Points	Lack of integration, lack of metrics, lack of requirements
Thales specific	No infrastructure mapping, no unified approach

Table 6.1: Summarized findings of the case studies

A summary of the findings from the case studies can be found in Table 6.1. During the case studies, different levels of sophistication were identified between the different organisations, ranging from basic implementation of BCM to advanced BCM strategies encompassing the entire organisation with further transformation. One of the main goals following the literature study was to identify the criteria used to assess the infrastructure in BCM at an organisation. Respondents were asked which criteria they use, followed by a discussion about criteria found in the literature and their perceived usefulness for the organisation in assessing the impact. From these interviews, six main criteria have been identified, *financial impact*, *operational impact*, *regulatory impact*, *reputational impact*, *third-party impact* and *security impact*.

Next to identifying and assessing continuity management, it is also essential to see how organisations evaluate their strategies. This is required to understand if the chosen strategy and solution can achieve

the intended continuity goal as without any measurable success indicators, it becomes challenging to assess the current continuity capabilities and improve over time. Organisations currently make use of three KPI's: *RTO*, *RPO*, and *MTPD*. Organisations consider *RPO* and *RTO* as fundamentals and see them as KPI's that have been around for a long time already and might be a bit dated if those are the only ones used.

Lastly, pain points have been identified related to continuity management and the successful assessment and evaluation of assets. Notably, here are the *lack of integration* of continuity management into the core of the organisation. *Insufficient continuity criteria & metrics* underline this problem further, and in combination with a *lack of requirements* shows that organisations are struggling to gain a clear overview of the intended and actual capabilities of the continuity team and their approach.

CONTINUITY MANAGEMENT ASSESSMENT METHOD

The following chapter introduces the final continuity management method developed after validating the draft method. The BCM assessment method introduced in this chapter consists of the identified stages of BCM, a list of impact criteria from theory and practise, criticality levels and their definition, a list of key performance indicators and a practical iterative method on how all of these can be used in the context of a BCM assessment.

7.1 CONTINUITY MANAGEMENT STAGES IN A ORGANIZATION

This section describes the view an organisation could take with its BCM strategy and how it can evolve to improve its BCM capabilities over time, visualised in Figure 7.1. The first two stages have been seen in the interviewee organisation and on their account, indicating that they are planning to move from stage one to stage two. The last stage has been designed from the interview information and in collaboration with Thales. Continuity management is often an afterthought in projects due to budget constraints, putting the organisation at risk. In the last stage, this problem is resolved by including continuity as a core requirement for projects.

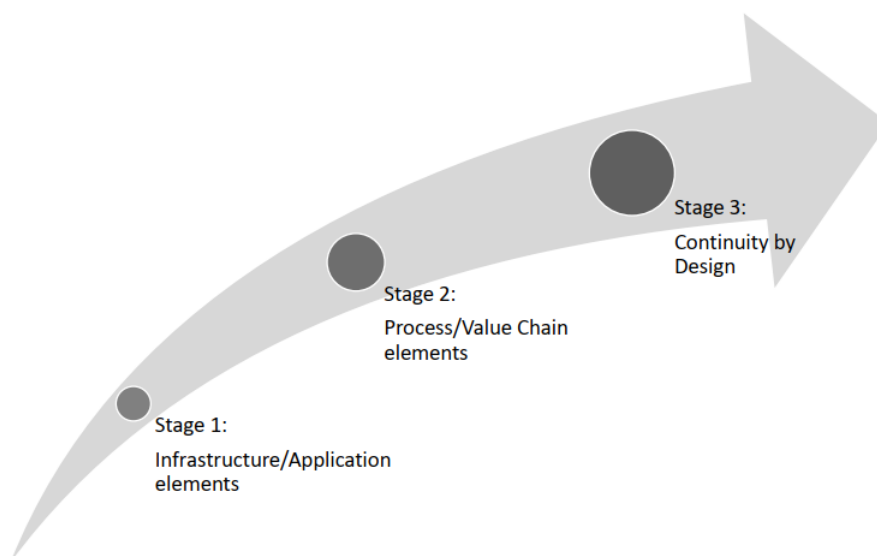


Figure 7.1: Stages in BCM

7.1.1 *Stage 1: Infrastructure/Application View*

Stage 1 is concerned with an infrastructure/application viewpoint. This is the first state big and established organisations will be in and a state that an organisation should start with. Here the organisations focus on the infrastructure such as buildings, employees, hardware and the like in an isolated manner. This creates the baseline for the BCM strategy and is a crucial part of establishing core continuity capabilities.

If an organisation cannot recover their (physical) infrastructure on a basic level, any more advanced recovery strategies building upon the infrastructure can not be performed. For example, the organisation must recover a power outage at their data centre in an acceptable time frame before thinking about recovering specific applications or hardware in the data centre. It turns into an iterative approach to take more detailed views on the infrastructure.

Following the infrastructure view, still in the same stage, is the application view. These stages have been combined into a single stage as they do not have very many differences from their approach and only differ in the level of detail. At the application level, the organisation considers the separate applications or services they are running, or less IT-specific, the machines used in a production line, in an isolated view. This means that an application is viewed as a single element that is not connected to others.

This view allows for a more detailed assessment of applications, services and machines. They are evaluated according to the iterative method in [Section 7.2](#) and give the organisation an understanding of how impactful a disruption on a specific asset/process is. However, in this stage, the assessment does not allow for a proper understanding of the application, service or machine in the context of the organisational processes. Therefore, the next big step in the BCM strategy of an organisation should be the shift to a value chain/process-based view.

7.1.2 *Stage 2: Process/Value Chain View*

The second stage requires the organisation to shift from an isolated assessment towards a value-based view. When in the first stage, an application was looked at in an isolated view, in a value chain based view, the organisation identifies their value chains. The application is only a tiny part of a more extensive process that generates value for the organisation. The process view allows for a better understanding of the organisation's interdependencies of assets/processes. Moreover, it also enables the organisation to identify and prioritise the processes that generate the most value for the organisation. Even though

this shift towards a value chain focus is already mentioned for continuity management by Herbane et al. [12] but is not yet widely used in IT by organisations. However, supply chain companies or even the supply chain departments in organisations naturally consider the whole process. Hence the name supply "chain", as a disruption in the supply chain will disrupt the complete process. This means that the knowledge on how to look at a process view is already present in some companies but is not transferred into IT and continuity management.

7.1.3 Stage 3: *Continuity by design*

The last stage, termed "*Continuity by design*", aims to establish continuity management as a core process in an organisation and remove it as an afterthought. Continuity by design requires changes in most parts of the organisation and might take a long time to implement correctly. The first change is, of course, the buy-in of management into the concept and relevance of continuity. Here the first two stages will help establish proper assessment, evaluation and reporting of the impact of a disruption and the BCM capabilities of the organisation. Only with a clear understanding of what generates value for an organisation and how the disruption to those value chains impacts the organisation can management make an informed decision.

After a clear picture is established, continuity by design has to be implemented into the organisation's core process. This involves the infrastructure development making sure that continuity is a consideration in every new hardware that is getting implemented; application development and implementation must consider continuity during the design phase of new software, and any significant changes to systems, processes, or infrastructure should be communicated beforehand and the impact on the continuity evaluated.

Organisations that do not have continuity management plans and systems can start directly on this level. This would allow them to use all the benefits from ensuring continuity from the get-go. However, this might only be possible for smaller and younger organisations as it is expected that more extensive and older organisations have already an enterprise infrastructure in place, and changes will therefore be more difficult.

Moreover, as long as the organisation cannot successfully explain the value of such a solution and the potential impact of a disruption in case of a disaster, it will be difficult to convince management to invest in such solutions. IT projects are often lacking funding and have a limited budget leading to BCM being dropped due to costs.

7.2 ITERATIVE ASSESSMENT METHOD

As this project aims to provide a practical approach to assessing BCM, an iterative assessment method is proposed that can be used during all three stages and most departments of an organisation. It follows closely to the Plan-Do-Check-Act cycle, as seen in Figure 7.2, a known approach for carrying out change and should be repeated again and again for continuous improvement. The cycle consists of four steps, *Assess*, *Design*, *Implement* and *Validate*.

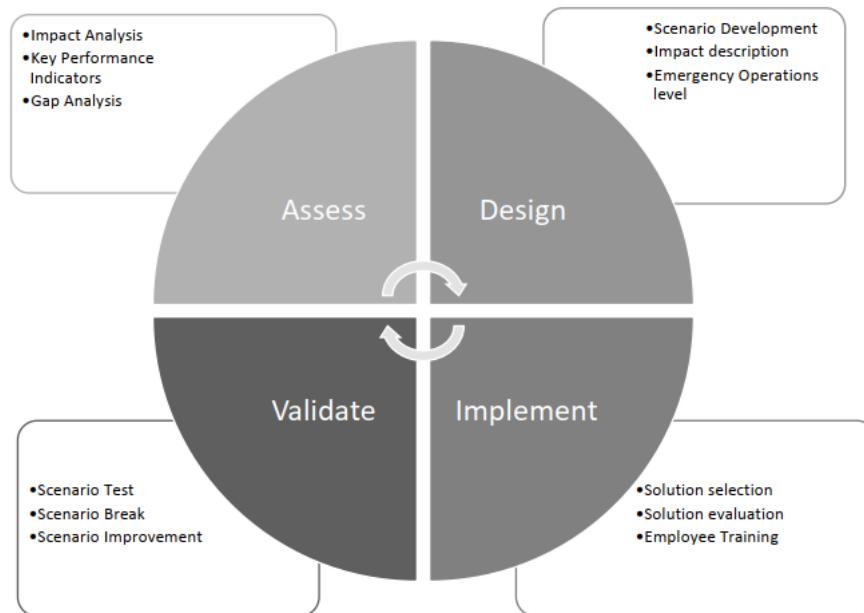


Figure 7.2: Method

7.2.1 Assess

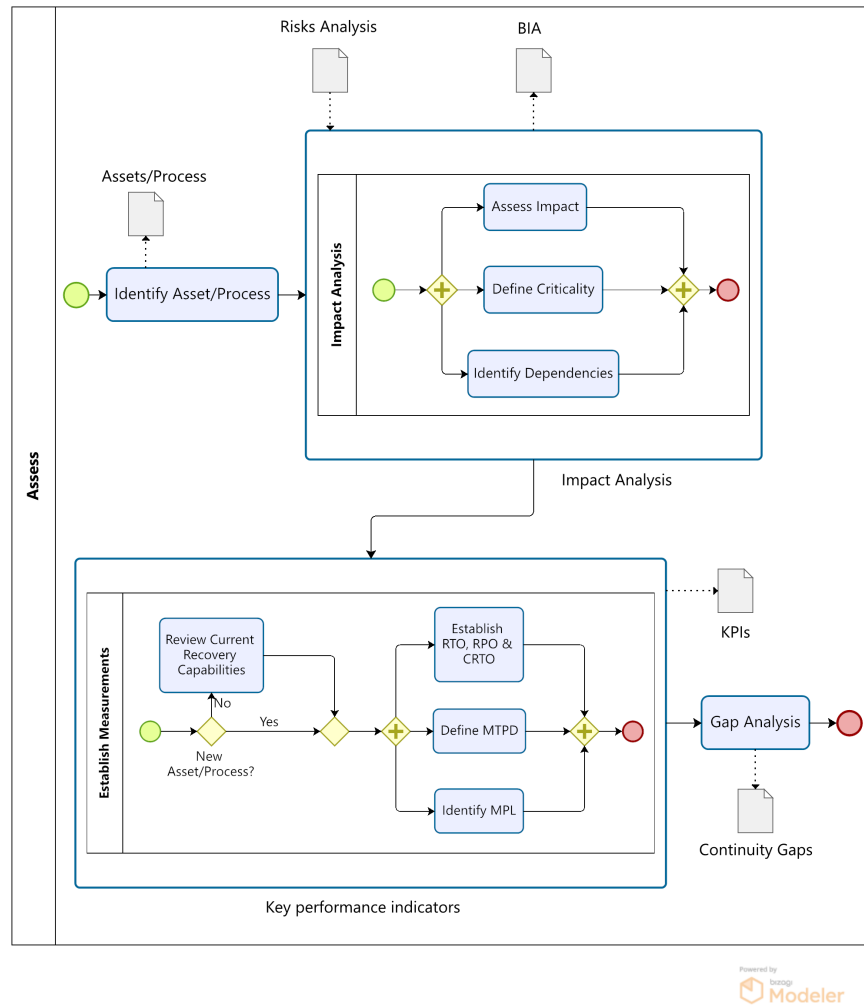


Figure 7.3: Assess assets steps

The first step, *Assess* that can be seen in Figure 7.3 is based on an impact-based assessment, where we are trying to quantify what the potential damage of disruption is. It all should start with investigating the risk assessment already done for the IT infrastructure. This analysis can give the first idea of asset/processes at risk and allows for the first consideration of risks the organisation wants to mitigate beforehand. A company does not have to make continuity plans for risk, if and only if the risk can fully be mitigated. However, a risk analysis will only consider known risks, while in continuity management, it is not known beforehand which disaster will strike, and the continuity plans must cover many different possibilities. Therefore, the idea is to protect the organisation's most valuable asset/processes.

Following, the BIA, as proposed by Cerullo [10], is the next step in the assessment to quantify the impact based on different criteria. This is in line with the ISO-22301:2019 standard [24]. The first set of criteria gives a good understanding of the impact of a disruption. Not all criteria have to be used by an organisation for each asset, and they should only be used if the organisation considers them relevant for the asset.

7.2.1.1 Impact Criteria

During this research, five critical impact criteria were identified and used in different capacities by organisations to assess the impact of potential disruption. These criteria are of qualitative and quantitative nature. Each criterion should be evaluated on a 5-point/level scale [34]; this allows for a good enough differentiation between different impact levels while not enabling too detailed differentiation where it becomes more challenging to distinguish at which level the impact should reside. An example with impact levels can be seen in Table 7.1. These are only suggestions, and the values should be adapted to fit better for an organisation. These criteria are also linked to common enterprise risk that organisations might experience [49] e.g. *financial risk*, *operational risk*, *strategic risk*, *information risk* and *compliance risk*.

- *Financial Impact:*

When assessing any asset in an organisation for continuity, one of the first criteria that an organisation should use is *financial impact*. As a result, the goal is to establish the direct financial loss due to the disruption of an asset. E.g. a disruption of a server due to hardware failure will have a direct financial loss on the damaged hardware that has to be replaced, a broken machine in a production line.

- *Operational Impact:*

Next to the pure financial damage that can be evaluated, disruption will often affect the daily operations of an organisation and their employees. Employees might not perform when systems are not working and employee hours are lost. These losses can add up quickly, depending on the disruption and can cause substantial damage to an organisation. Different approaches can be taken here; the organisation can estimate the total employee hours lost on its own, or if wanting to express it in terms of monetary loss, the organisation can multiply it by an average hourly rate. The company can gain a rough estimate of the financial loss due to interruption in the daily operations as indicated in Section 6.5.2 and proposed by Rabbani [39] as one of the potential costs.

- *Regulatory Impact:*
Regulatory investigations might be performed by oversight bodies whenever substantial unexpected disruptions occur, especially in the banking or defence sector. This can lead to fines that must be paid or contractual obligations that are missed. Services provided to external parties are a primary concern here as there are often contractual obligations and penalties defined if these are not met.
- *Reputational Impact:*
Whenever a disruption occurs, the reputation of the organisation can be damaged. This can be a loss of reputation in the public eye, the regulators, government or a loss of reputation toward their clients.
- *Third-Party Impact:*
With more and more complex systems in organisations and the shift to outsourcing tasks, third parties are often highly involved in the processes of other organisations. Organisations must be aware that when using a third party, they give away some control of their system; hence, when a disruption happens, they might not act independently and wait for the third party to resolve the problem. While this can be problematic, it does not have to be as third parties have continuity plans. However, the organisation should always know how a third party is involved in a particular process.

Three more criteria were identified next to these five criteria during the interviews. Therefore, these criteria are more specific and are not fit for all organisations or all assets but should not be forgotten and can be used when deemed necessary as those criteria cover areas that can lead to more significant impact.

- *Health/Safety Impact:*
Certain disruptions can impact the safety and health of employees, physically and mentally, and should be considered in areas where necessary.
- *Employee Impact:*
Another consideration should be taken when the impact will affect the organisation's employees. This could be, for example, confidential information about employees being exposed.
- *Customer Impact:*
When having customer-facing processes or services, the organisation has to evaluate, together with the customer, what the impact is for the customer.

CRITERIA	IMPACT LEVEL	TIME
Financial Impact	A: More than €10 Million	
	B: Between €1 Million and €10 Million	
	C: Between €100 thousand and €1 Million	
	D: Between €10 thousand and €100 thousand	
	E: Less than 10 thousand	
Operational Impact	A: More than 1000 employee hours	
	B: Between 500 and 1.000 employee hours	
	C: Between 100 and 500 employee hours	
	D: Between 10 and 100 employee hours	
	E: Less than 10 employee hours	
Third-Party Impact	A: Fully outsourced to third party with no own control	
	B: Third party is required for execution of a critical activity	
	C: Third party involved in execution of an activity with no alternative available	
	D: Third party involved in execution of an activity but alternative available	
	E: No third party involved	
Regulatory Impact	A: Major governmental sanctions expected	
	B: Minor governmental sanctions expected	
	C: Breach of regulation	
	D: Breach of internal policies	
	E: No regulatory impact	
Reputational Impact	A: Major Negative exposure by major media	
	B: Minor Negative exposure by major media	
	C: Negative exposure by minor media	
	D: Negative exposure by word of mouth	
	E: No negative publicity	

Table 7.1: List of Criteria with example impact levels

Next to those eight impact criteria, two more measures were identified that do not describe impact but, if compromised, will affect the assets that organisations could use to assess assets.

- *Security risk:*
With security risk, especially when looking at IT, the organisation should assess their asset/processes concerning confidentiality, integrity, and availability, putting it into its security context. The example security risk levels are based on Thales five security levels used to classify data.
- *Speed of Onset:*
Lastly, the speed of onset can be used as an assessment criterion. Speed of Onset is used to describe the speed at which the disruption will unfold. Some disruptions will take longer and might be detected and prevented before they materialise; others might onset within seconds. E. g. the disruption of a production machine might be noticed immediately, but due to some left-over stock, the problem will only materialise when the stock is empty, and the whole production line can not progress anymore due to a lack of parts.

7.2.1.2 Criticality levels

Due to many organisations using criticality levels when talking about the importance of an asset to the organisation but not having a general definition of what the criticality levels mean, we define four different criticality levels identified during interviews. The first three levels are based on Wiboonrats [45] proposed levels in combination with the common use of criticality in Thales and the other interviewed organisations. These criticality levels build upon each other; an asset should only be part of one of the first three levels. The highest level, *mission-critical*, covers all aspects that *critical* covers and more on top. *Time-critical* should be seen as a optional level that can be added onto any asset regardless of which level it has been assigned to.

- *Mission-Critical/Business-Critical:*
Any system that is fundamentally necessary for the organisation to exist - a system that must be available 24/7.
- *Critical:*
Any system that the organisation requires during the daily operations to generate value. If interrupted, substantial damage to the value of the organisation occurs. A system that has to be available From Mo - Fr/9 - 17h
- *Non-Critical:*
Any system that is not in one of the first two categories or has an identified, functional and independent alternative can be used during a disruption.
- *Time-Critical:*
A particular category should be assigned to any system with a time-based criticality change. E. g. a salary systems criticality rises on the day the salaries have to be paid and falls off directly after again.

7.2.1.3 Key Performance Indicators

Next to assessing the organisation's assets/processes, it is also important to define key performance indicators. Not only to understand the current capabilities for ensuring continuity are but also to identify gaps between the current state and the intended state. Therefore, 7 KPI's are set below that should be used to keep track of capabilities and goals. The KPI's can also be seen in Figure 7.4 in relation to each other during a disruption.

- *RTO / Recovery Time Actual (RTA)*
Recovery time describes the time it takes for the organisation to recover from a disruption back into full operation before substantial damage occurs. Recover time *objective* is the intended

time the organisation wants to achieve with their continuity strategy for a specific asset. Recovery time *actual* is the actual time the organisation needs to recover from a disruption of a specific asset. This measurement can only be established during functional testing of the scenario plan. This measurement represents the actual capabilities of the organisation. The RTO describes the desired time to recovery and should always be smaller than the Maximum Tolerable Time of Disruption (MTPD).

RTO can be directly linked to the *financial impact* and *operational impact*. Both will likely increase with longer recovery times and must be weighed against each other.

- *RPO / Recovery Point Actual (RPA)*

Recovery point describes the amount of (data) loss the organisation can take from a disruption before substantial damage occurs. Recover point *objective* is the intended maximum loss the organisation wants to achieve with their continuity strategy for a specific asset. Recovery point *actual* is the actual loss the organisation will endure from a disruption of a specific asset. This measurement can only be established during functional testing of the scenario plan. This measurement represents the actual capabilities of the organisation.

RPO can be related to *Speed of Onset*, as it determines the time between the actual time of disruption and the organisation becoming aware of the disruption will relate to the amount of data loss for the organisation.

- *Cumulative Recovery Time Objective (CRTO)*

Cumulative recovery time describes the cumulative time frame it takes the organisation to recover a specific asset. Due to interconnectivity and dependencies of systems, it is likely that when an asset is disrupted, it will negatively affect other systems and take them down. These systems must be brought back in order. To have a clear understanding of how long it realistically takes for a system to be recovered, it needs to be clear which systems must be recovered first. Therefore, CRTO is a good addition as a measurement for organisations to keep track of this.

- *Maximum Tolerable Time of Disruption*

As discussed in Section 6.6.3, the MTPD lacks a practical definition for most organizations [17]. Therefore, we want to establish it here as a concrete red line. The MTPD is the absolute maximum must have time for recovery. This time should never be reached, and organisations must know what they should do when this red line is crossed. This can mean that an organisation will request external help to solve the disruption, end recovery attempts, try a clean setup, and accept lost data.

- *Minimum Level of Performance (MLP)*

Recovery does not happen instantaneously and not to 100%. Therefore, it becomes crucial to define what level of performance the organisation wants to achieve during recovery. This means MLP describes the Minimum level of services acceptable to the organisations to achieve its business objectives during a disruption.

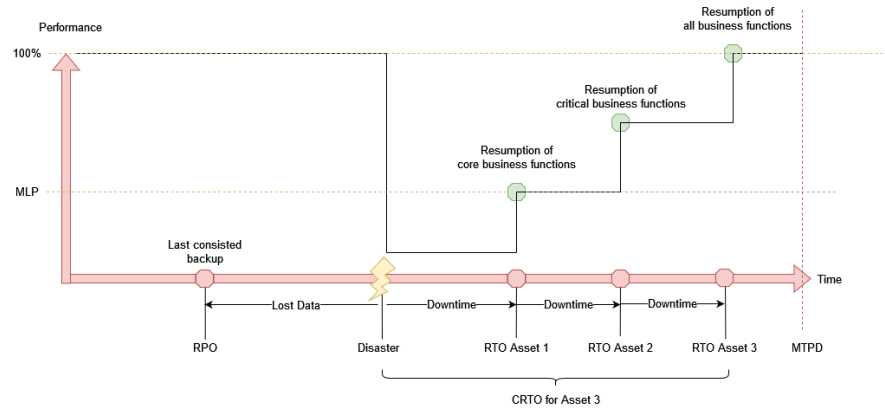


Figure 7.4: BCM key performance indicators

Lastly, it is also essential for the organisation to formally define the time measure for the KPI's start. General advice is to consider the time in these KPI's to start as soon as the organisation is aware of a disruption. This seems obvious, however during the interviews, it became clear that organisations just assumed everyone considers it this way without actually defining when it starts. It is up to the organisation to decide on this, state it clearly in relevant documents and communicate it to the teams responsible for continuity management.

7.2.2 Design

While the first step was focused on assessing and quantifying the impact, the next step *design*, see Figure 7.5, focuses on prioritising and describing impact for a scenario plan. This step is based on the planning stage of the IT disaster recovery life cycle from the ISO 27031:2011 [25]. Beginning with the selection of the most critical asset/process, therefore all *mission-critical* assets/processes will be looked at first. To distinguish even further, we look at the established criteria and rank them based on the levels assigned, A till E. E.g. the more impact criteria are assigned with A, the higher it should be prioritised, continuing this system down the list.

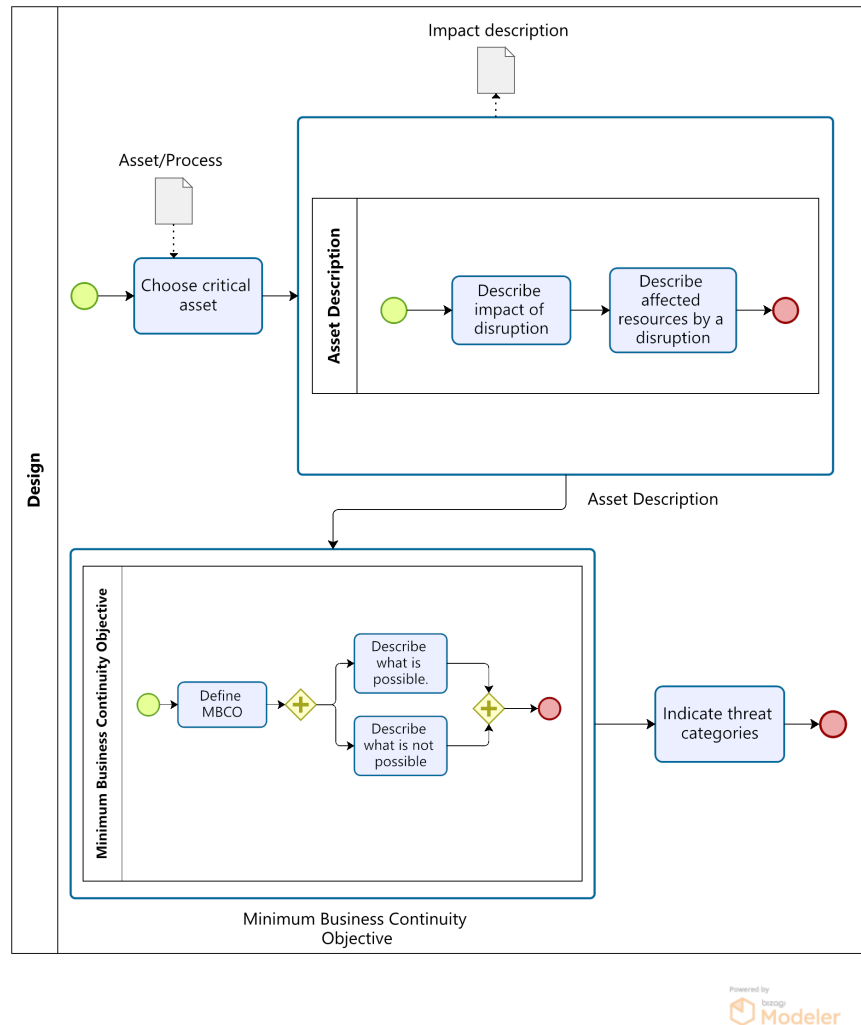


Figure 7.5: Design scenario steps

For each element, the first step should be to use the quantified criteria and express the total impact and the affected resources on a 5-level scale [34]. Each criterion is ranked on a 5-level scale, A to E. The highest level is taken as the overall level, or the organisation combines all criteria into one level, giving the asset an overall importance ranking. Afterwards, the emergency operations level should be defined and possible threat categories assigned. Lastly, the whole information collection must be combined into a scenario plan or an asset impact document.

Impact summary

Next to the quantified impact, we determined that a written summary of the impact adds to the scenario development. Someone reading this plan and only looking at the quantified impact might not understand the problem with a disruption of the asset and how it impacts

the organisation in practice. Therefore, a written summary from the process or asset owner can provide valuable information, allowing for a quicker and better understanding of the impact on the organisational goals.

Resource summary

Like the impact summary, a Resource summary tried to describe the affected resources in a written way, allowing for a quick understanding of potentially affected assets/processes. Asset owners can provide more information about the relevance of certain assets to a process or service. Some assets might be more relevant for the core business that is unclear when looking at the quantified impact. Resource and impact summary have been added as it was indicated during interviews that next to a quantified impact, it should also be necessary to explain the impact in a short description where critical assumptions or information can be communicated.

Minimum Business Continuity Objective (MBCO)

MBCO describe what is and what is not possible at the bare minimum operational level for the organisation [7]. During scenario development, the organisation must determine the emergency operations level for an asset/process. To establish this, the organisation should define what is and what is not possible at this level during a disruption. This can mean that specific compliance requirements can not be fulfilled during an emergency state. While such a level would not be perfect for the organisation, they would have a clear picture of their capabilities during a disruption.

Threat Categories

This continuity management assessment method is based mainly on impact and less on threats, and most organisations indicated that they also consider their continuity management to be based mainly on impact. It still can be helpful to indicate what kind of threats a scenario can cover and what kind of threats would not be covered by the scenario. A scenario plan for IT servers might cover digital attacks such as ransomware with a well designed backup strategy but would be less suited to cover environmental disasters such as floods. Therefore, it should be made clear what a scenario covers and where gaps still exist.

Possible threat categories can be: *Malware, Hacking, Social Engineering, Environmental, Misuse, Error* or *Physical*. This list is not exhaustive and only provides a small set of threat categories seen in Table 4.3.

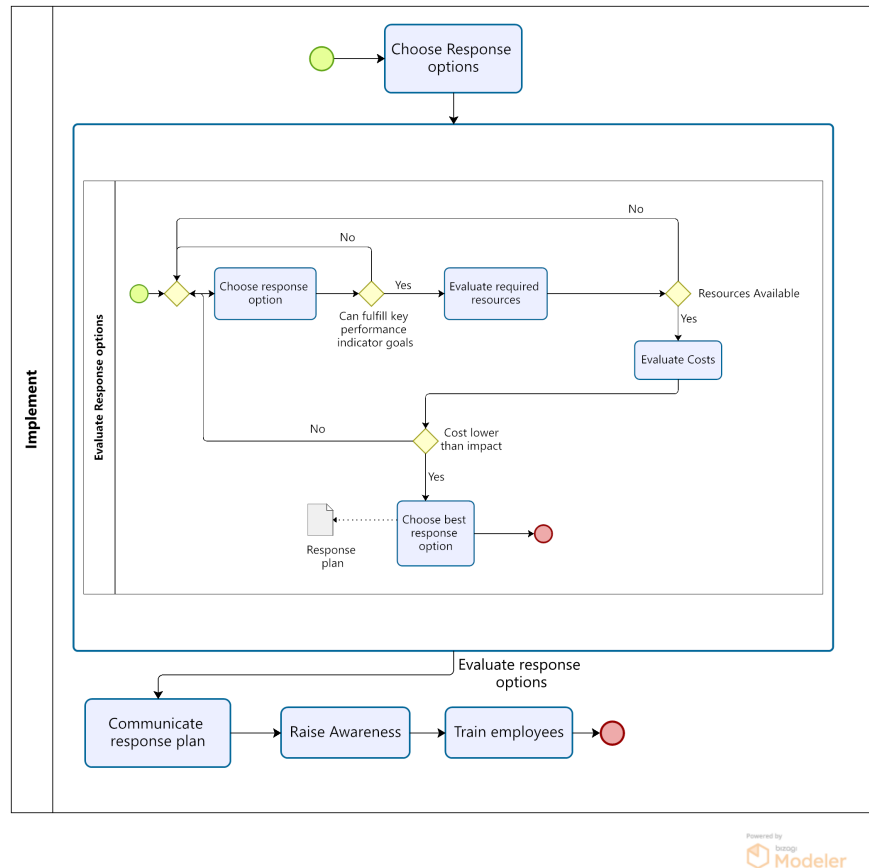
7.2.3 *Implement*

Figure 7.6: Implement scenario steps

Response options

When choosing potential solutions to implement the continuity plans for asset/processes, many different approaches can be taken, and they vary wildly depending on the asset to protect. The process can be seen in Figure 7.6. While the following list is not exhaustive, it gives a general overview of the potential approaches.

- *Fail over*: One of the more simple solutions to limit the impact of a disruption is having a failover available. A copy of the disrupted asset can take over the task of the affected asset, and almost no downtime will occur. While this solution is straightforward, it is also very impractical to employ for every asset as this would mean having everything at least twice. However, for big mission-critical assets/processes like data centres, a failover backup site is a common and proven approach yet costly.

- *Alternate independent procedure*: Another approach to limit the impact of a disruption is to have an alternative procedure to perform the same task. This alternative must be independent of the primary procedure and not affected by the same disruption.
- *Manual processing*: Manual processing can be a reasonable solution for smaller tasks that might be ordinarily automated. E. g. Moving a part on the production line to the next station can potentially be done by hand; a text editor can temporarily be replaced by pen and paper.
- *Third party/outsourcing*: Outsourcing the solution is another approach to limit the impact. Here a service contract is made with a third party to perform specific tasks for the organisation during a disruption. E. g. Taking overproduction of a specific part of the machine on-site is broken to ensure that the supply chain can continue. It is also possible to outsource the complete BCM responsibility to a third party. This would then be considered a DRaaS where service-level agreements outline the requirements and possibilities.
- *Do nothing*: Lastly, the organisation can also do nothing. Sometimes, the solutions will be more expensive than the impact of the disruption. When that is the case, the organisation can accept the damage of the complete disruption and follow a regular recovery plan to bring everything back to normal.

Evaluate

Following a selection of possible solutions, an evaluation based on the KPI's and criteria has to be performed. This includes the goals that can be achieved with the selected solutions and if they meet the minimum criteria for the organisation, but also feasibility for successful implementation has to be considered. Every solution requires specific resources, and the organisation must make sure that these resources are available.

Communicate

As a next step, following the lack of communication expressed during interviews, see also Section 6.7.1, is the communication of the intended plan with relevant stakeholders. It is essential to get back to the process owner and employees who would be affected by disruption and discuss the intended recovery strategy to reconfirm that all requirements of the Business Unit (BU) are met. The plan also has to be communicated with the crisis management team responsible for the recovery of the asset. Roles and escalation chains have to be set and maintained.

Awareness & Training

To end this step, the employees have to be trained [10]. On the one

hand, the crisis management has to be trained for the new plan, made aware of any changes if the plan was adopted, and assumptions made. ON the other hand, to raise employees' general awareness, this can also be used to explain to employees what is done to ensure that the services can be recovered, who is responsible for it, and the maximum planned downtime. This will help employees to understand the disruptions better and raises their awareness about such problems when encountering them.

7.2.4 Validate

In the last phase, *validate*, the designed scenario plan must be validated for the KPI's. The process can be found in Figure 7.7. Firstly, the scenario plan must be tested, and afterwards, the team should try to break their designed scenario. This can then be used to establish the RTA and RPA for the asset and identify gaps between existing capabilities and intended capabilities, and the scenario can be improved upon after that until the objectives are achieved.

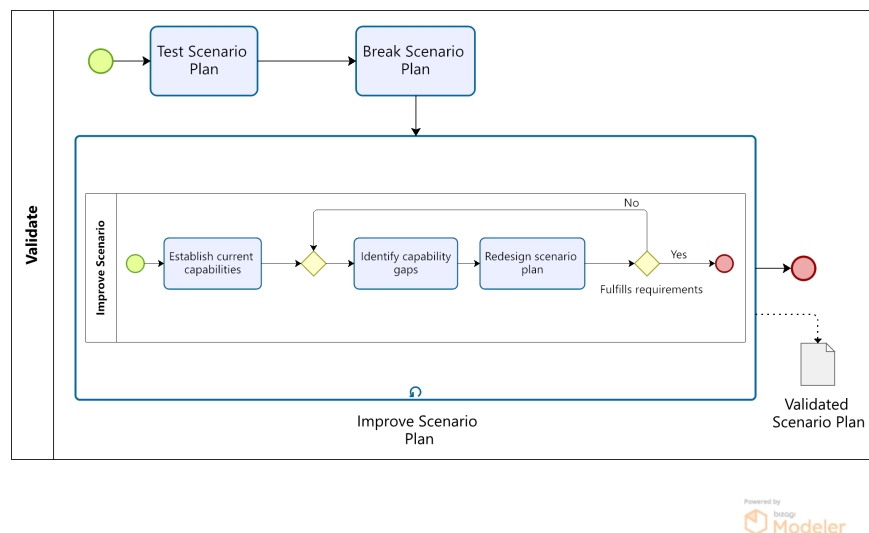


Figure 7.7: Validate scenario steps

Testing & Exercising

As a critical indicator of a successful BCP, all plans should be tested and regularly evaluated [10, 25]. This ensures that the plan remains relevant and employees are trained in successfully following the plan.

Testing & exercising the scenario can be done via tabletop exercises or practical disaster simulations. While the former is more convenient and more accessible for the organisation and can identify critical problems with the approach, the latter provides a better real-world envi-

ronment and forces the plan to be performed and questioned.

Especially for BCP that are aimed at mission-critical asset/processes where it is challenging to perform a real-world test without actual interruption daily operations, we advise to perform these tests as close to real-world conditions as possible as a minor disruption during the daily operation is drastically better than a significant disruption and a plan that does not perform as intended.

Break

Breaking the scenario plan is an important next step in ensuring its usefulness. During scenario development, the designers might make many assumptions during this phase, especially when testing via tabletop exercises they happen in a perfect environment. Many of these assumptions might not be true during a disaster, and the systems might not act as assumed during the exercise. E.g. If during a disaster with the loss of IT, the first step is to gather the disaster plan, and this is stored only at the server, the emergency team is not able to get the recovery plans anymore due to the unintended assumption during the tabletop exercise that the plans are available. Hence, breaking the scenario after it has been tested successfully is a crucial step in the validation of the BCP.

Improve

Lastly, all knowledge gained during the validation and testing of the BCP can be used to improve the individual plan but also can be used to update other plans following a similar approach. This is the continuous improvement step in the PDCA cycle seen in Figure 2.1.

Maintain

After all plans are checked, the plans can be used to limit the impact of a disruption. However, now that the plan is considered done, the plans must be routinely checked if they still follow the best practices in the organisation, if all assumptions made are still valid and if relevant roles are up to date.

Whenever changes are made on the asset/process, the relevant BCP have to be revisited and potentially adapted. These changes should again be communicated with all relevant stakeholders. Substantial changes to the plan should require a test to be performed again and a time frame for the next test set up.

Remarks

After all this, it is essential to always keep in mind that no written plan can foresee all contingencies; decisions against the plan might have to be made based on experience or often common sense during a disruption.

7.3 ENABLE THE CRISIS MANAGEMENT TEAM

As last part of this method is a mandatory scenario that every organisation must have to ensure their continuity capabilities.

Ever [BCP](#) relies on the Crisis Management Team/Recovery team to be able to recover from a disruption. Therefore, this team must always be able to operate. If disruptions prevented the crisis management team from performing their recovery operation, the organisation would be helpless, and the disaster could not be mitigated, limited or recovered from.

The team must be reachable at any point via two separate independent channels to prevent a disaster from impacting the communication. Recovery plans must be available at multiple locations and best follow the 3-2-1-1 backup rule, see [Section 4.7.1.1](#), to have access to the plans regardless of the disaster. Moreover, contact details and communication orders must be kept at hand and updated to inform the right people as soon as possible.

VALIDATION

This chapter summarises the validation interviews and the adjustments made to the method based on feedback received. As seen in Table 8.1, four experts in (Business) Continuity Management were interviewed during this phase.

Position	Expertise	Experience
IT Security Officer - Bank NL	IT security, disaster recovery, continuity management	6 years
Continuity manager - Bank GER	continuity management, crisis management in critical infrastructure	11 years
Supply Chain manager - Electronics production	supply chain, IT management, disaster prevention	7 years
CIO - Thales Netherlands	IT security, Enterprise architecture, leadership	14 years

Table 8.1: Experts interviewed for validation

8.1 IT SECURITY OFFICER

The first expert to be interviewed was an IT security officer at a dutch bank with six years of experience in IT security, disaster recovery and continuity management. The interviewee said that while continuity management is a critical process for banks and enforced due to governmental regulation for a long time, only in the last few years, with the fast growth of cyber-attacks did other larger organisations start investing money and resources into continuity management, often without having the necessary infrastructure to support it properly. Since the interviewee was actively involved in continuity management at the bank, he provided general feedback on the different parts of the method.

8.1.1 Stages

The respondent said that organisations would be in many different stages of continuity management. While some might have very advanced systems where the whole process is considered, most are probably not at this point yet. Looking at the stages identified and defined in this research, he highlighted that they are pretty rudimentary and high-level. However, he thinks this high level will provide enough context for the organisation to understand the high-level development steps to increase continuity capabilities. While the exact levels might be slightly different for every organization, they capture the three main components, *Infrastructure/application, process/value chain* and *continuity by design*.

8.1.2 *Criteria*

The first version of the method contained many different criteria, some very specific ones. The respondent thought it might be better to generalise them on similar concepts found in other areas like risk management. Moreover, he noted that limiting the criteria assessment to a set of levels would be beneficial, allowing for differentiation between impact levels on criteria and often preventing splitting impact levels.

Following, the Criticality levels were considered good, but he also indicated that they are struggling with defining them properly but thought that the definitions would fit well and that it is good to be defined in the first place. The expert agreed that this is often missing and gives organisations a good start, and they can still redefine them if they think it is necessary.

8.1.3 *KPI's*

The expert mostly agreed with the key performance indicator and their description of the method. He mentioned that it would be good to combine *objective* and *actual* KPI's as they are closely related. Furthermore, the KPI *MLP* was seen as a great addition to the set of KPI's. However, he also mentioned that it might be challenging, if not outright impossible, for an organisation to determine it well. The other KPI's were seen as valuable and well-fitting.

8.1.4 *Method*

The respondent considered the method to be well done. He mentioned that the method should not be too complicated when used in practice. Furthermore, the split into the four different tasks, *assess*, *design*, *implement* and *validate* follow known patterns that most people would easily recognise and therefore would feel more comfortable performing as they would know how they would work.

8.1.5 *Scenarios*

Lastly, he highly agreed with the idea to add the scenario of *Ensuring Crisis Management* to the method as the first scenario every organisation has to consider. It will allow the organisation and the crisis management team to gain some first experience in designing scenarios, but it will also ensure that they are somewhat prepared for the worst-case and therefore be able to solve disasters in the first place.

8.2 CONTINUITY MANAGER

The second interview was held with the Continuity manager at a German bank. While he has been only one year at this bank, he has more than ten years of experience in continuity management and crisis management in the critical infrastructure sector. With his extensive knowledge, especially about critical infrastructure, the interview mainly focused on those areas.

8.2.1 Stages

The expert indicated that renaming *phases/steps* to *stages* would be better as this would make it more straightforward that these build upon each other but are not time-based increments. He agreed that the first stage that every organisation should take is on the *hardware* level as they have to be able to recover those before anything else. However, he thought that it might be better to rename *hardware* to *infrastructure* and combine it with *application* in this method as they are very similar and only *process/value chain* indicates a new level of maturity that should be separate. He stressed that the *process* view is slowly crawling into other areas of IT and that IT departments must consider applications and infrastructure in the processes they are used in instead of isolated objects.

Lastly, he thought that *continuity by design* might be less of a stage that an organisation goes through but a long term change that encompasses many parts of the organisation. However, he agreed that this is a logical next step that organisations can take to improve their capabilities across departments.

8.2.2 Criteria

The respondent focused on the definitions of criticality levels in this method concerning the criteria. He agreed that organisations have to define their criticality levels in a meaningful way that can be used consistently. He disagreed with the idea of directly basing it on the financial impact or any monetary value as these are often difficult to estimate and vary too widely to be helpful. It might be more beneficial to base them on availability and alternatives to mitigate the impact. Therefore, the criticality levels were based on availability 24/7, working hours, or not at all.

Additionally, he supported the idea of a time-based criticality level that could be used for systems that change criticality on known times and allow for more control for the organisation as this information might be lost otherwise in documents.

The expert confirmed that the criteria found are partially used at his organisation but missing other criteria. He indicated that criteria

like *Health/Safety Impact*, *Employee Impact* and *Customer Impact* should be included as well as they are often seen in the critical infrastructure sector and can be of value to an organisation. These have been added as additional criteria for organisations to use. He agreed with limiting the criteria to a scale and thought that a simple 5-level scale would provide enough depth to differentiate without giving too much room, preventing organisations from splitting criteria levels too much.

8.2.3 KPI's

He supported the KPI's found and used in this method. He also agrees with the previous respondent that it will be challenging to establish the [MLP](#) in an organisation. [MTPD](#) was seen by him as a good change, as this is an indicator used in his organisation for a long time without any actual use as it mostly matched the [RTO](#) and did not provide any more information to the organisation. He also supports the idea of [CRTO](#) as a separate measurement as the [RTO](#) values were often just considered for the single asset and not for the complete process it might take to recover.

8.2.4 Method

The respondent considered the method approach to be lacking surrounding context in the early iterations and mentioned that steps like communicating the plans to the employees and crisis teams should be added to the approach. Moreover, he pointed out that raising awareness was often brought up to increase security during an internal discussion for security. He saw this as a good idea to include into the method for increasing awareness about continuity management, not only on a fundamental level but also to use this time to raise the awareness of the crisis team about the new plans, assumptions and procedures.

8.2.5 Scenarios

He agreed with the previous respondents that ensuring the ability to act for the crisis management team is one of the most crucial scenarios that an organisation should consider. Therefore, he supports this scenario as part of the method itself but would not add more fixed scenarios to it as every organisation would have a different focus afterwards.

8.3 SUPPLY CHAIN MANAGER

The third interview was conducted with a supply chain manager at a production company in the Netherlands. With three years of experience in the supply chain and four years in IT, he provided valuable feedback on the method and stages. He stated that it became more evident to him that IT needs to change towards a process and value-based perspective due to his switch from IT to supply chain and the difference of looking at an isolated object in IT to a process/supply chain view when considering a production line.

8.3.1 *Stages*

The interviewee supported the idea of the previous respondent for renaming the stages, giving it a more precise description. Concerning the stages themselves, he stated that it heavily depends on the organisation and their current processes and that there might be too much difference between their current state and the proposed state in the method to be implemented by large organisations quickly. While minor changes like assessing assets via more and new criteria and KPI's can be implemented regardless of the state of the organisation. A shift towards a value/process-based view would need to encompass every department of the organisation and would require much time, making it difficult for larger organisations. Nonetheless, due to his switch into the supply chain, he agrees that this is the right way forward for organisations and IT departments.

Regarding the first stage, the respondent thought it might be unnecessary as any organisation with some continuity management processes in place would be at the first stage. He noted that it was logical that an organisation would start on the basic level of its infrastructure to ensure continuity.

Concerning the *continuity by design* stage, he thought that the more the organisation could integrate continuity into the design of their enterprise infrastructure, the fewer problems they will most likely encounter via disruptions. However, this change will also take a long time as it affects the organisation's processes and the employees and how they perform their work.

8.3.2 *Criteria*

The expert indicated that the criteria proposed to provide an excellent collection to start with for an organisation are closely related to risk assessment concepts and are easily understood by most in an IT department. He highlighted that these criteria should also not be too specific and detailed as they will be looked at in a yearly cycle or when a disaster happens. While there will be enough time during the

normal review, during a disaster, these criteria must be understood as quick as possible by the crisis management team.

He pointed out the *third party* criteria that are easily seen in a supply chain when material deliveries are delayed, or shortages exist. However, they are often missed in IT as it might not always be directly clear if a service is provided internally from the IT unit or a third party or if any component in the process relies on a third party in any way.

He also thought that *Speed of Onset* should be a criterion to consider. Coming from the supply chain, some disruptions materialise immediately while others will only occur a few days later, like a production line with a few days of stock available that can bridge the disruption of a machine. Therefore, *Speed of Onset* has been added to the optional criteria as such disruptions could also occur in IT.

8.3.3 KPI's

When asked about the key performance indicators proposed in the method, the interviewee thought that *RTO* & *RPO* would remain the two most relevant indicators to measure and design solutions with. Looking at *MLP*, he agreed that organisations should be able to specify what their expected recovery level is during a disaster as well as indicate what tasks can be performed at this level and what is not possible at that time. He also agreed with defining when these measurements are started with a disruption; he had an idea that his organisation starts measuring as soon as the disruption is known to the organisation but was not sure if this was defined somewhere; therefore, he sees this as a good addition in the approach and eliminating the chance that people expect it differently.

8.3.4 Method

While the expert thought that the method was sound and agreed with the comments made by the previous respondents, he mentioned that he was missing a connection to threats in the model. It was not clear what kind of threat would lead to such an impact for him. He proposed adding threat categories to the method so that during the assessment, it can be made clear what kind of threats could lead to such an impact and see what kind of threats are not covered or would affect it. These categories have then been set to *Malware*, *Hacking*, *Social Engineering*, *Environmental*, *Misuse*, *Error* or *Physical*.

Moreover, he indicated that the plan would be tested in the method, and his addition would include a next step where the team would attempt to break the plan. This was brought up as members would make unconscious assumptions that are not visible in the plan. Therefore, the next step after testing a plan should be to break it to find the

plan's flaws. Additionally, he mentioned that it should be clear that the plan produced at the end might still not be able to be used in its total capacity as it should be expected that something was missed during the creation of the plan.

8.3.5 *Scenarios*

For scenarios, he indicated that he is not very involved in the design of the supply chain scenarios. When asked about the scenario of ensuring the crisis management team can do their work, he agreed that they invest substantial resources into ensuring that their team of engineers can repair any production line problem if necessary and that multiple independent teams are available to handle this task. However, he noted that this was not always the case during the pandemic and that there have been moments where a qualified person would not have been available on short notice to limit the impact of substantial disruption.

8.4 CHIEF INFORMATION OFFICER

The last interview was conducted with the CIO of Thales Netherlands. This interviewee provided a high-level view in the IT department and technical feedback due to his previous roles in the IT department at Thales and the industry.

8.4.1 *Stages*

The respondent liked the idea of providing organisations with a structured approach to short-term goals that increase continuity capabilities and a long-term outlook on how the development should go further along over time. This would allow organisations to plan further ahead and implement necessary changes to the culture and processes of an organisation to increase the resilience against disasters in the long term.

8.4.2 *Criteria*

He highlighted and urged that *reputation*, even if challenging to measure success, is one of the essential criteria for organisations in the bigger picture. Under the slogan "Building a future we can all trust", ensuring a good reputation and ensuring trust becomes very important. An organisation that is not able to handle disruptions appropriately will lose trust. This criterion should be one of the main criteria, therefore.

8.4.3 KPI's

The CIO supports the approach of measuring the capabilities via KPI's as measuring is one of the critical elements in understanding organisations do the problem and not enough in continuity management to gain a proper understanding of the problem. He agrees that relying only on [RTO](#) and [RPO](#) is not enough and approves the addition and value of [CRTO](#). Moreover, he thought that establishing [MTPD](#) as a red line to escalate the problem further is a good approach, especially when in a crisis. On the other hand, while he understands the intention behind the [MLP](#), he considers this to be one of the last parts an organisation should and would look at when establishing their continuity management capabilities.

8.4.4 Method

The respondent mentioned that the method lacked input from the risk analysis and indicated that this should be added to use the knowledge gained through it to mitigate risk. Moreover, he argued that for each identified asset, the probability of disruption should be estimated to allow for better decision making and prioritisation. Nevertheless, he understood that the method is more aimed at establishing the impact of any disruption and that estimating the likelihood that any disruption occurs on a specific asset might be challenging.

Generally, more organisations will have to look at their continuity approach and how they will assess the impact of disruption as a significant disruption will happen at some point. Nevertheless, not only the processes and assessment but also the management practices and investments into ensuring continuity will have to be evaluated and progressing towards *continuity by design* appears to be a first step forward.

8.4.5 Scenarios

The interviewee agreed that designing scenarios to ensure that the most important assets are covered presents a significant challenge to organisations as it is impossible to consider every way an asset could be disrupted. Focusing on the most critical assets based on criticality and value generation is crucial, and changes are already happening. Nevertheless, they all are based on the notion that the crisis management team can intervene when a disaster strikes and becomes the core of the strategy to ensure continuity - ensuring that the team can work when a disaster strike is a significant part, and he supports the idea of designing one of the first scenarios around that.

8.5 SUMMARY

Category	Findings
Stages	Provide good long term goals for organisations allowing for incremental improvements of continuity capabilities
KPIs	<p>A valuable addition to the current continuity assessment practices.</p> <p>Allowing for quantitative reporting to upper management and better argumentation for future investments into continuity management.</p> <p>Solely relying on RTO & RPO as KPI's has been deemed insufficient.</p>
Criteria	Quantification of the impact is considered great next step towards a better understanding of the severity of a disruption to a organisation.
Method	The proposed method provides a good addition to the current continuity management standards Communication is still the most lacking steps in continuity management.
Scenario	Ensuring the ability of the Crisis management team to be able to perform the recovery and execute the plan has been accepted as a great addition and starting point for scenario development for organisations.

Table 8.2: Summarized findings of the validation interviews

The interviews led to different changes of the method, such as re-naming *phases* to *stages* as well as additions to the list of criteria and the ranking of those. Furthermore, the method adopted to the Plan-Do-Check-Act approach uses more general concepts.

Overall, the respondents agreed with the method's general approach and the stages that an organisation could take to improve their capabilities over time. However, these later stages are seen by most as very difficult to actualise and implement in larger organisations, especially *continuity by design*.

Overall, the respondents judged the list criteria positively, with some additional criteria identified during the interviews. Meaning that the proposed list of criteria sufficiently evaluates the impact of a disruption, and continuity managers and higher management alike seemed to be optimistic about the approach to quantify the problem better.

Most respondents indicated that additional KPI's like [MLP](#) and [MTPD](#) are excellent additions to [RTO](#) and [RPO](#) in this method to evaluate the impact further and measure the performance of the organisation. However, it would take significant resources of the organisation to

establish these new KPI's for each asset or process and see them as a later step in improving their continuity approach.

Another important conclusion is that *Communication* is one of the most lacking steps in current approaches and that Communication should also not only happen inside the continuity departments but also should communicate with outside departments. Lastly, the addition of a worst-case scenario that every organisation should consider first has been accepted well by the respondents and supported the idea.

8.5.1 *Usability and Implementation*

Almost all interviewees considered the method, criteria, and KPI's to be a good and useful addition to their current continuity assessment approach. They would allow the departments to have better quantitative reporting abilities and enable the teams to provide better arguments to management for future investment into continuity management.

However most organisations consider the later stages to be either very difficult to implement throughout the organisations or consider them a long term project that needs to be planned accordingly.

The additional criteria and KPI's are considered easy to implement and some of the interviewees already indicated that some of the criteria will be implemented in the next assessment round. Additionally, the KPI's used by the organisations are being revisited, properly defined and new KPI's as mentioned in this research added.

DEMONSTRATION

9.1 CASE SELECTION

In this section, we will provide two examples of the method applied. The first example will look at the Printed Circuit Board (PCB) plating line at Thales. Once looking at the machine is isolated and once as a process trying to highlight why a process-based view provides an entirely different picture of an impact than an isolated picture. Secondly, we will look at the process of remote access to the network, a process that, in the time of working-from-home, is used by many employees.

9.2 PCB PLATING MACHINE

For this example, we will look at the PCB plating machine, once isolated and once as the entire process trying to assess the impact of a disruption of the machine. The machine is a single production unit in the PCB production line at Thales.

9.2.1 *Process*

The process to create an electronic board is complicated and involves many steps and machines, as seen in Figure 9.1. This Figure is only an example of a PCB production process and does not show the actual PCB process at Thales but is sufficient for the following sample assessment. It can be seen that each step builds upon each other and that disruption would impact all following machines but also, after some time, the machines that perform tasks before the plating line. For this assessment, we focus on the plating line in the Figure seen as step 10.

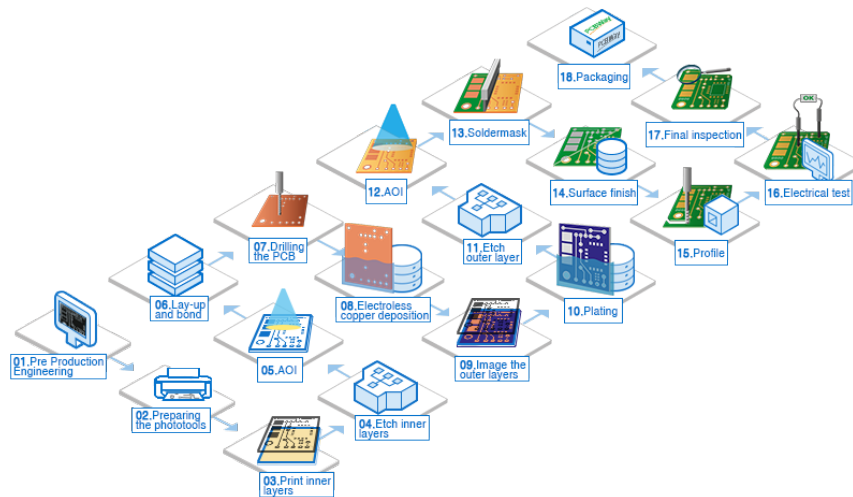


Figure 9.1: PCB production process - PCBWay [51]

9.2.2 Applied Model

9.2.2.1 Criteria

At first, we will look at the financial impact of a disruption on the machine. If the machine has a total failure and can not be repaired by the engineers of Thales, it can be seen as a significant disruption. When looking at the costs to replace such a machine, it is estimated by the engineers to be around €1 Million, and there is no difference here when looking at it isolated or as an asset in the production chain. Regardless of our perspective, the machine would need to be replaced for the production to continue.

However, significant differences can be spotted when looking at the operational impact. The machine itself is operated by around five people, meaning every day the machine is out of operation, there might be a loss of around 40 employee hours when not reassigned to other tasks. When we are now looking at the complete process that the machine is part of, and we know from Thales that this machine does not have a replacement or alternative, a disruption will lead to a standstill of the complete PCB production line as soon as the remaining stock runs out. This is estimated to be after around one week. If viewing this disruption as part of the whole production line, it will now affect around 50 employees and not only 5, leading to 400 employee hours lost every working day the machine is out of operation. This is a significant increase of lost productivity for employees and certainly increases the urgency of the disruption compared to taking the view of the isolated machine.

Next, when looking at the third party impact on the machine itself, we might not see a big problem overall and consider no third party to be involved in the production. When considering the complete pro-

cess of the production line for third party impact, we notice that third parties provide the material via contracts and regular deliveries. If the production process is now interrupted at one of the machines and material can not be processed anymore, impact from third parties may occur due to material deliveries being rejected due to full stock. This should be seen, therefore, as *Third party involved in execution of activity but alternative available*.

With a significant disruption comes scrutiny about the processes to prevent these disruptions, and regulatory measures would be put into place to mitigate this disruption in the future. As Thales produces PCB's for the internal use of producing radar systems, this would also impact the defence sector of the Netherlands. Therefore, we can expect some minor governmental sanctions following such a significant disruption. This could force Thales to ensure that such a disruption would not happen again, or worse, the government would look for another supplier, reducing the revenue Thales could generate.

Due to a disruption on the production line, the reputation of Thales for reliably delivering and producing products will drop. Customers of Thales will have less trust in Thales being able to deliver in time. Thales being active in the defence sector can also lead to a loss of trust by the country's defence organs. This might become public and would create significant harmful exposure by major media. We do not see a reasonable impact on Thales' security due to a disruption on the production line; however, it could be argued that it would affect the country's security if the production line is out of business for too long.

Considering the speed of onset as an essential criterion in a supply chain, when considering the machine in an isolated setting, a breakdown of the machine would be noticed immediately in full effect for the machine alone. However, when considering the whole production process, the breakdown would also be noticed immediately, but the full impact due to the stop of the whole production line would only materialise after one week when the stock ran out. The full impact here would be noticed later, but the impact would be considerably more significant than in the isolated setting.

Lastly, we should look at the impact of the customers of Thales, the PCB's are used mostly internally, but some are also sold to external third parties. Both can and should be considered customers of the process and would be impacted by a disruption. Of course, this would only be noticeable when considering the complete production process and not an isolated machine. Customers relying on the production of PCB's by Thales would need to find alternative products when the production line is down. The internal customers would be impacted as they could not continue building their radar systems, leading to a cascading problem down the production chain, causing disruptions in other departments and processes. Therefore, we consider the impact

on customers to be *Major impact on customers* as cascading problems could quickly impact wider parts of the organisation.

9.2.2.2 Criticality

Considering the criticality of the machine and process as one of the production processes, it is a core part of the Thales business and should therefore be considered *critical*. There is no need for the machine to run 24/7, including the weekend, so we do not consider the process to be *mission critical*.

9.2.3 Key performance Indicators

When deciding on key performance indicators for such a significant disruption, it is essential to try and establish realistic indicators that can be achieved. While in IT, recovery times might be short; short recovery times are often unfeasible in a supply chain with physical machines.

9.2.3.1 RTO / RPO

A full recovery would only be achieved after the machine was replaced and production resumed for the Recovery Time Objective. Knowing from discussing that acquiring and installing such a machine would take at least six months, any RTO below that is not feasible. Trying to be conservative during the estimations and assuming that these times could likely be higher, an RTO of 8 months seems reasonable to assume for such disruption if everything goes according to plan. There is no data loss or generalising the concept of RTO to a production line, and no parts would need to be redone a step or would need to be disposed of; establishing an RPO makes little sense here.

9.2.3.2 MTPD / MPL

With an RTO of 8 months, the MTPD must be placed reasonable further away, determining the time that should not be crossed for recovering the process of PCB production. With placing the MTPD to 12 months, it is roughly twice the time that is estimated to replace the machine and get back into production again. After 12 months, the organisation should look for alternative solutions. E.g. permanently outsourcing the production or investing and modernising the production line with more readily available machines.

The MLP and MBO for the production of PCB's should allow the organisation to at least cover the internal demand of the other departments. No estimate will be made here as it is unknown how much of the production is used internally. However, as the organisation itself

can only achieve this if the machine is replaced and back into production, other solutions should be considered until this moment is reached. E. g. outsourcing the production step itself to a third party or outsourcing the steps up and including the broken machine so that the new production process starts after the impacted machine.

9.2.4 *Impact & Resource Summary*

Next would be the summary of the impact, partially already provided in the previous sections, describing the problems and impact of a disruption. Notably, the extended downtime that would be expected due to such disruption is first. 6+ months before a replacement can be procured is a significant time frame to affect the production line and impact more than just the production line at Thales and external customers. These would not receive their products anymore, and the supplier as Thales would not be able to use their parts anymore, and the deliveries have to be stopped, contracts would be impacted, and clients might be lost. Hence, Thales should see this disruption as unacceptable, and actions must be taken to prevent such problems, as is already done with preventive maintenance.

9.2.5 *Threat Categories*

When considering threat categories involved in such a disruption and could be limited with a solution, we primarily look at physical threats. Misuse, Error, Physical and to some extent, the environmental impact could all be limited with the response options below. Each threat could lead to the machine breaking, and a replacement option would need to be in order.

Such solutions would only partially cover threats like malware, hacking, or social engineering. Failovers or alternatives would potentially not be impacted by such a disruption and could therefore still perform their duty; however, it could also be the case that the alternatives or failover machines are impacted by the same malware and would be unusable.

9.2.6 *Results & Solutions*

From the comparison, see table 9.1, we can see that there are many similarities in the assessment between an isolated machine and the complete process there are noticeable differences in the operational impact, third party impact and customer impact. Especially the operational impact shows a big difference and brings a substantial cost to the front that might not be caught immediately and the third-party impact that could easily be forgotten. If not already done, the organisation should establish their current actual capabilities to limit the

impact of such a disruption. At the end of this step, the organisation would be at the beginning of the *Implement* step.

9.2.6.1 *Response options*

Considering the criteria and indicators established above, it is also interesting to look at potential response options and argue for and against them in this setting. Which solution to choose can be based on multiple factors: The main decision criteria are most often the cost of the solution; in general, the solution should cost less than the impact it limits. This can change if costs are not the main driver for the organisation. If the organisation does not have the main driver for such a decision, the impact assessment can be used, choosing the criteria with the highest impact levels as decision criteria to decide for or against a solution.

Fail over: The first response option would be a failover solution; this would require a second machine to be in place in the production line that can take over the task of the disrupted machine. This is the most simple solution that can be used to prevent such a disruption. It does, however, require to have enough space in the production hall to place such an extra machine, as well as it should then be considered if not every machine the production chain should have a failover machine as any of the other machines could have a complete breakdown too, ending with two complete production lines. This can be a potential solution similar to the active/active data centre, where both data centres are active and handle a part of the load, but each on their own cannot handle 100%.

Manual processing: While many tasks that are fulfilled by machines or software might be done by manual processing, production lines like these would expose the employees to chemicals and would drastically increase the risk of harming the health of the employees and should not be considered as a viable solution to a disruption

Third party/outsourcing: Another approach towards this problem is the usage of a third party. The third party could take over the PCB production of the organisation for a limited time until the replacement machine has been installed and is back in production. If arranged beforehand, this is a feasible solution as the third party would have kept capacity available; if this is arranged after the disaster, it might not be possible to find a supplier that can produce the required product. For this approach, multiple ways are possible too; the third party could take over the entire production and deliver the end product, take over the step of the lost machine, or perform all the steps up till the broken machine.

Do nothing: Lastly, the organisation can accept the disruption and do nothing else until the replacement machine is acquired and back into production. This should only be considered if all other solutions are more expensive than not doing anything. Even then, the organi-

Criteria	Isolated machine	Production Line
Financial Impact	Between €1 Million and €10 Million	Between €1 Million and €10 Million
Operational Impact	Between 10 and 100 employee hours/h	Between 100 and 500 employee hours/h
Third-Party Impact	No third party involved	Third party involved in execution of an activity but alternative available
Regulatory Impact	Minor governmental sanctions expected	Minor governmental sanctions expected
Reputational Impact	Major negative exposure by major media	Major negative exposure by major media
Security risk	No security risk	No security risk
Speed of Onset	Immediately	Immediately/ Full Impact: after 1 Week
Customer Impact	None	Major impact on customers

Table 9.1: Example assessment of PCB production line

sation must consider what this would do to its reputation as doing nothing might put a bad light on them.

9.3 CONCLUSION

Based on the assessment above, even though more detailed information is not accessible to us, Thales could decide which action is to be taken to limit the impact of a disruption. Considering that the financial and operational impact is very high and the *RTO* for the machine is long, it is unfeasible to *Do nothing*, *Manual processing* is also unfeasible for the time of the *RTO* and would expose employees unnecessarily to dangerous chemicals. Therefore, *Fail over* or *Outsourcing* are the two most viable options.

Fail over requires Thales to have enough space to place or store another machine on site. However, this would only cover this machine and not the whole process. To protect the whole process, every machine that could be a single point of failure would require a failover machine to ensure the whole process is protected. This can make sense when Thales expects their demand for *PCB*'s to grow enough to warrant another machine and then could run both machines at the same time with less than full capacity.

Outsourcing would require Thales to find a *PCB* producer nearby and enter into a Service agreement with them, ensuring that the third party would take over the production of the *PCB*'s for the time of the disruption. Thales would need to make sure that the supplier fulfils all requirements to be allowed to produce *PCB*'s for military parts and that Thales is allowed to share the plans with the third party. Nonetheless, this solution seems to be the most viable one because it is easier implemented, and the operational costs are expected to be lower than acquiring and maintaining a second *PCB* production line.

9.4 REMOTE ACCESS

To provide an example demonstration of this method in IT, we will use it to assess the impact of a remote access service used by many organisations to log into the organisation remotely with general information related to Thales and their impact. Remote Access via VPN

allows users to access the organisation's network anytime, anywhere to accommodate flexible work arrangements, travelling employees or working from home during a pandemic. This process, however, involves a lot more than just the VPN gateway that the employees faces, including but not limited to Access & Identity Management System (AIM), Firewall or Active Directory (AD), see Figure 9.2. If any of the underlying systems or hardware is disrupted, it will also affect the remote access process of the organisation.

9.4.1 Process

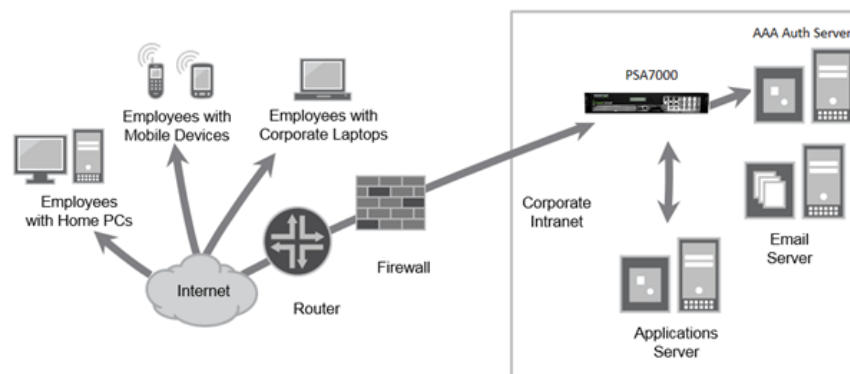


Figure 9.2: Simple remote access [50]

The user will log into their laptop or phone and connect to the organisation's network. The user provides username and password and additional multi-factor authentication methods, such as software token, phone-as-a-token or context-based methods, will need to be performed. This authentication will then pass through the firewall, and the AIM has to verify the user. After the user has identified themselves, they will access the network and perform their daily work.

If the user can not gain remote access to the network, they will not be able to continue their work, and therefore the organisation will have a productivity loss. As this disruption would most likely affect many employees, especially during the current work-from-home time, the damage to the organisation could be substantial. Not only can the VPN gateway itself be affected by the disruption, but the underlying systems can also impact users from gaining remote access. A disruption of the AIM or the AD will also impact the remote access process and prevent employees from connecting to the network. Moreover, system administrators might also use remote access to resolve problems; when the remote access is impacted, the system administrators must be on-site to resolve the issue.

9.4.2 *Applied Method*

As we start with an asset already, we will skip identifying assets. In the first step, we will look at the impact criteria and try to assess the potential impact of a disruption to the process of "gaining remote access to the network".

9.4.2.1 *Criteria*

As a first criterion, we look at the pure financial damage of such a disruption. Assuming that an underlying hardware failure does not cause it, no direct financial damage would occur as nothing would need to be replaced. However, when looking at the operational impact, it becomes clear that the organisation will have many employees unable to work while the disruption persists. Thales Netherlands has roughly 2.200 employees; from discussions, we learned that roughly [redacted] of those work in production and would be on-site. From the remaining [redacted] around [redacted] work from home, when no pandemic is going on, this lowers to around [redacted] employees working from home. Therefore, we can estimate that Thales Netherlands will lose between [redacted] employee hours per hour. Moreover, the process is disrupted if the disruption requires the employees to come to the office again. There might be a loss of a full working day (8h). We do not expect any regulatory impact due to a disruption of the process in general, as this process would mainly affect the employees of Thales. However, we expect some reputational impact, not necessarily from the outside but from the employees themselves. The more frequent and frequent such disruptions occur, the more annoyed employees will become, and trust in the organisation to provide the services required to perform their work will drop. Here we would consider it a "negative reputation due to word of mouth", employees might vent their frustration to colleagues about the problems.

Looking at Third parties involved in the process, the multi-factor authentication methods, firewalls and endpoint protection are often provided by external parties, and this as well can disrupt the process if the third party has a disruption of their service. However, the authentication methods can also act offline in most cases and would not pose a significant cause for disruption, but it should not be forgotten. Therefore, "a Third party is involved in executing an activity with no alternative available" will be chosen. Receiving support during a disruption can take longer than expected depending on the third party, and the [RTO](#) might be missed.

Lastly, looking at security impact, the remote access process presents the way into the organisation's internal network and puts the information stored there at risk. Therefore, a disruption of the remote access process can put confidential information at risk and should be treated as such.

9.4.2.2 *Criticality*

Next, we have to assess the criticality of the process. This process can be considered *critical*: It is not necessary to run 24/7 and on the weekend but is required during the regular working hours on a working day. However, if many employees who connect to Thales NL are abroad or in different time zones, the service might also be needed during the weekends. While *going to the office* can be seen as an alternative, this might not always be possible due to other circumstances like pandemics or other plans that relied on home-office for the employee. However, if the disruptions continued for multiple days, employees would most likely come to the office again. Hence, a few lengthy disruptions might be less impactful than many minor disruptions with the same total time. Moreover, a time criticality can be indicated: At the beginning of work hours, most employees will try to connect to the network, and therefore the process is more critical at that time, also shortly after lunch when most employees come back, they will have to reconnect to the network. These two points in time can be seen as most critical for the process as disruption will affect most employees.

9.4.3 *Key performance Indicators*

When establishing key performance indicators, we can only establish the goal indicators and not the actual capabilities that the organisation has as we do not know Thales current capabilities for this process. We will therefore focus on [RTO](#), [RPO](#), [MTPD](#) and [MLP](#).

9.4.3.1 [RTO](#) / [RPO](#)

We are first going to look at the [RPO](#): With a disruption of the VPN gateway for remote access, no actual data loss is to be expected. Hence a long [RPO](#) of multiple days can be justified. However, if data is lost or corrupted that the VPN gateway uses, such as configuration files, a recovery point of 24h is achievable due to automated daily backups.

While potential data loss of 24h might be annoying, it would not present substantial damage to the organisation; on the other hand, a [RTO](#) of 24h would mean that remote employees would not be able to perform their work for a full day. Due to the remote access being a critical element of the organisation, and a loss of [redacted] employee hours lost for each hour the system is down, a [RTO](#) of 2 hours during working hours, should be aimed to limit the impact of the disruption to at most [redacted] lost hours.

9.4.3.2 MTPD / MLP

The **MTPD** should be the red line when the organisation not only loses a substantial amount of money but also admits to not being in control of the disruption or unable to solve the disruption without external help. This gives a precise time when the organisation has to escalate the problem. To gain remote access to the organisation's network, we would set this to 1 week after the disruption. This gives the organisation enough time to solve the problem by themselves; however, the damage solely caused by lost productivity will be significant enough to warrant an escalation of the problem.

MLP & MBCO gives us an idea of what should be possible at the first level of recovery for a process. The minimum level of performance for the remote access process should allow employees to gain access to the network again. This might require a staggered login approach from the employees or a queuing system to mitigate the overloading of the recovered capabilities. This does not require lost data to be recovered already but mainly allows the employees to access the network and applications. Even with only 10% of the regular performance, employees should log in and perform non-load-heavy tasks. E. g. viewing and editing documents might be possible, while video conferencing might be locked until the system is fully recovered again to prevent overloading the systems.

9.4.4 Impact & Resource summary

Next would be the summary of the impact, partially already provided in the previous sections, describing the problems and impact of a disruption. A disruption of the remote access would have drastic consequences for the employees' productivity, relying on the secure connection to the organisation's network. Notably for this asset is the time criticality at the beginning of the working day and shortly after lunchtime. During these times, the impact of a disruption is expected to be higher due to more employees being affected. On the other hand, many short disruptions might be more impactful due to the behaviour of employees than a few lengthy disruptions.

9.4.5 Threat Categories

When considering threat categories involved in such a disruption and could be limited with a solution, we need to consider almost all current threat categories, but each response option might only cover a part of the threats. E. g. environmental threats like a flood or an earthquake could be mitigated with a failover response in a different location.

9.4.6 Results & Solutions

From the assessment, we can see that the operational impact can become quite prominent in little time. As remote access affects many employees on any given day, leading to losses, there is a financial incentive to limit the disruptions. From discussions, we know that currently, remote access is impacted for around [redacted] hours in a year. A solution that would reduce this impact either by providing alternative means or reducing the downtime should not cost more than [redacted] per hours reduction in a year. Otherwise, the solution would cost more than the impact is limiting.

9.4.6.1 Response options

As this process has many different components that could be affected, there are also many different ways to go around and limit the impact each could have on the organisation, some being more feasible than others.

Fail over: Failover again would mean that for each component, a replacement would be available that could be used during a disruption. Systems like the AD and AIM might already have failovers in place as they are the backbone of larger organisations. Systems for generating tokens or creating the secure tunnel into the network could be affected, and a failover could take over during a disruption.

Alternate independent procedure: Another approach is to implement an alternative, independent procedure. This could involve a separate way to generate tokens only when a disaster prevents employees from generating tokens. If it affects the software that creates the secure connection to the network, a similar approach can be taken, and an alternative secure network connection service is used again only when a disaster prevents employees from connecting. If such a disaster strikes one of the underlying systems required for verifying the user's identity and rights, an alternative procedure would involve having a second AIM system in place.

Manual processing: Manually processing the connection requests might be a possibility when the number of requests is meagre but does not present a viable solution for the organisation when they consider it a disaster. Hence, this approach is not suitable for such a disaster.

Third party/outsourcing: Another option is the involvement of a third party to take over handling remote access when a disruption has occurred in the organisation. This could be a full outsourcing with a *as a Service* concept, relying entirely on the third party during a disruption.

Do nothing: As the last option, the organisation could do nothing to limit the damage of the disruption. If any of the above solutions would cost more each year than the total damage done by such disruptions in a year, it is financially not beneficial for the organisation.

Criteria	Remote Access
Financial Impact	E: Less than 10 thousand
Operational Impact	A: More than 1000 employee hours/h
Third-Party Impact	C: Third party is involved in executing an activity with no alternative available
Regulatory Impact	E: No regulatory impact
Reputational Impact	D: Negative reputation due to word of mouth
Security risk	Confidential information at risk
Criticality	Critical
Time Criticality	Beginning of work day (8am) & after lunch break (1pm)
MTPD	1 Week
MLP	Allow for staggered login

Table 9.2: Example assessment of remote access

to implement any more measures. This should be regularly evaluated to ensure that the situation has not changed.

9.5 CONCLUSION

Following the assessment, Thales should decide which action is to be taken to limit the impact of such a disruption. Considering that the operational impact is very high, the *RTO* for the process is very short. *Manual processing* is unfeasible for the size of Thales and the intended *RTO*. Hence, Thales should either consider a *Fail over* solution, *Outsource* the solution or *Do nothing*.

Do nothing The least favourite option is *Do nothing*. This option should only be chosen if all other options are deemed unreasonable, too expensive or otherwise not fitting.

Fail over & Alternate independent procedure Failover requires Thales to implement a failover remote access system. Here a decision about the scope must be made if including a failover option for software and hardware, should it only be a second instance on the same hardware and systems, potentially also being affected by disruption and therefore negating its use. If considering the IT software side, an alternative independent solution would not be affected by the same disruption, e. g. a different software or another VPN tunnel.

Outsourcing Outsourcing would require Thales to find/use a third party supplier and enter into a Service agreement with them, ensuring that the third party would take over the deployment and security of remote access systems completely or only during disruptions. Thales would need to ensure that the supplier fulfils all security requirements to be allowed.

DISCUSSION

10.1 IMPLICATIONS

This research aimed to identify criteria used to assess the impact of disruptions and provide a practical method to assess an organisation's assets structurally. In order to achieve this, we identified criteria and key performance indicators that are used and applicable to organisations, as well as collected common approaches and identified common pain points.

10.1.1 *Perspective of IT Business Continuity Management*

The proposed shift of perspective when evaluating and assessing IT assets for Business Continuity Management is based on the paper from Herbane et al.[12] published in 1997. While we have seen some large organisations use the value chain perspective, it is still not used in most larger organisations. While some interviewees would consider this to be unfeasible due to the size and complexity of the enterprise IT systems, others considered it a challenge and have implemented such an approach successfully over the last five years. This diverse approach has also been encountered in other areas of continuity management in the organisations during the research. Organisations should consider how they can transform their whole organisation at once and what approach to take and which benefits they could gain when having a value chain based assessment and increasing their understating of disruptions in their organisation. Despite the method and stages proposed in this thesis, the study also identified other pain points that organisations are struggling with within continuity management. It has become evident that soft controls such as communication and collaboration between teams/silos are essential to success. These soft controls will have the most notable impact in the long term when teams start to collaborate and communicate better.

10.1.2 *Quantifying the Impact of a disruption*

The results further suggest that most organisations have yet to sufficiently quantify the impact of disruptions for their continuity management systems. The use of criteria to quantify the impact of disruption increases the understanding of the organisation and allows to make more informed decisions when considering actions to limit the risk the organisation would be exposed. This stresses the need for a prac-

tical approach and criteria for organisations; current standards do not provide enough information to organisations so that they would be able to implement or improve their current continuity management systems on their own. Continuity Management experts agreed that organisations need to understand their assets better, how they provide value, and what the impact of a disruption on such an asset would mean for the organisation. Moreover, they support the notion that continuity management should become a base requirement for future organisations to stop current practices of pushing continuity management back due to budget constraints.

10.1.3 *The future of IT Business Continuity management*

With the rise of more and more cyber attacks on organisations, IT continuity management will gain more importance over time due to constant changes in enterprise systems and, therefore, a constant adaptation of continuity plans towards these new and different systems. This makes it important for organisations to have a clear understanding of their infrastructure, dependencies, and proper change management, allowing for the assessment of continuity management before implementation. These problems will also drive the implementation and further development of *continuity by design*. While organisations are still seeing this step as a challenge to implement in an organisation, it will allow organisations to stop chasing after the problem of continuity management and start being proactive in ensuring the continuity capabilities. Continuity capabilities should not decrease with the implementation of new systems but should be kept at least up to the current level. To start with *continuity by design*, organisations should perform organisational as well as technical changes, best in a pilot project in a small part of the organisation. Organisational changes can include employee training in continuity management similar to security training; this will raise the basic understanding of most employees in the organisation for continuity management.

10.2 VALIDITY

Validity refers to whether an indicator designed to measure a concept is actually measuring that concept. Yin [47] proposes four types of reliability and validity to be considered when performing a case study research. *Internal validity*, *external validity*, *construct validity* and *reliability*; these will be discussed in the following sections.

10.2.1 *Internal Validity*

Internal validity describes the cause-and-effect relationship established in the study to which the researcher can be confident that other factors cannot explain it [16].

The research draws causal conclusions on and for the criteria and method proposed making internal validity relevant for the research. Improving internal validity for a case study can be done by pattern matching or explanatory-building [16]. Pattern matching was applied by investigating multiple companies and identifying which criteria most have used and how they have been used. Analysing the interviews and coding the results allowed us to establish within-case and cross-case analysis. The internal validity is therefore ensured.

10.2.2 *External Validity*

External validity considers the domain to which research can be generalised [16]. According to Yin, [47], and Wieringa [46] using multiple case studies and applying replication logic allows for greater external validity and improves the generalisability. However, it is not possible to be sure of the external validity. The external validity of our research is limited by the number of companies studied in the case study, which is only a tiny number compared to all organisations using continuity management. Moreover, only companies from the Netherlands and Germany have been studied and therefore might be biased towards those countries and their approaches. While we can not guarantee full external validity, the methods and findings support a high degree of generalisability for companies of similar scale in the same countries.

10.2.3 *Construct Validity*

Construct validity concerns whether the correct operational measurements for the concepts to be studied have been established. In case studies, construct validity is seen as uncertain due to the subjective nature of collecting data and processing results [16].

The first concept to be studied in this research was concerned with the impact criteria used by organisations to assess their assets in IT. These criteria were collected and have a shared meaning by all organisations, and most had been seen in previous literature as well. Other concepts such as level of detail or stages were more difficult to measure and relied on the experience and judgement of the interviewee.

To ensure construct validity, Gibbert [16] encourages to *establish a clear chain of evidence* to allow readers to follow the process from initial research question to final conclusions and *triangulate* to adopt different perspectives. A clear chain of evidence has been established

using verbatim interview transcripts; however, due to almost only one interviewee per organisation, this limits the construct validity to some extent. On the other hand, we investigated multiple different organisations and sources of evidence that counteract the lack of interviewees. Furthermore, all participants could read their transcript before it was used for further research. Therefore, we can conclude that the two criteria by Gibbert have been fulfilled, but the limited evidence limits the construct validity to some extent.

10.2.4 *Reliability*

Reliability of research concerns the repeatability of said research by others with the same results. To achieve this, researchers should create case study protocols and create a case study database later on [47]. Due to the anonymity of the case study participant and confidentiality agreements with organisations, it is impossible to provide detailed information. While many different approaches have been seen in organisations, it is expected that another researcher would find similar criteria and methods as we found in our research when investigating similar organisations. This is supported by common criteria and processes found in most organisations; it is also expected that other researchers would find the organisations to be at similar phases as identified in this research.

10.3 QUALITY OF RESEARCH

While the previous sections discussed the quality of the case study analysis of data via validity and reliability. We also have to investigate the validity and reliability of the design research part. For that, we are looking at Hevner's [1] seven guidelines for design science research. See table 10.1.

Table 10.1: Guidelines for design science research by Hevner[1]

Guidelines	Description by Hevner	Our research
Design as Artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.	We are providing a list of impact criteria and KPIs as well as a practical method for assessing impact of assets
Problem Relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.	Business Continuity Management has been identified as a relevant business and security problem in the recent years.
Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.	The method and criteria have been evaluated with expert and sample implementations. However, a empirical validation has not been conducted.
Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.	This is one of the first studies in continuity management attempting to provide a practical assessment method for the quantification of the impact of disruptions in IT.
Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.	A semi-structured literature study was performed according to Kitchenham [28].
Design as a Search Process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.	A iterative approach during search and design was used to find the optimal artifact.
Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.	The research has been present to a group of Continuity experts/IT managers as well as higher management. The research will also be defended at the university in front of researchers in the field of Business Information Technology

CONCLUSION

11.1 RESEARCH QUESTIONS

This research aimed to investigate and identify a practical assessment approach for assets in continuity management. Secondly, it intended to investigate criteria and KPI's used in the assessment of assets in continuity management. Therefore, followed the main research question:

How can organisations assess their assets in practice in the context of IT business continuity management?

In order to answer this question, a semi-structured literature review, a case study, and sample implementation have been performed. The results have been evaluated with experts in continuity management and IT security. Three sub-questions have been formulated and answered in the following part to answer the main research question.

What criteria are used by organizations in practice and which criteria are organizations missing?

The case study and literature study have shown that there was no consistency in the criteria used by organisations in practice. Combining the most used criteria in collaboration with expert opinions lead to five main criteria: *Financial Impact*, *Operational Impact*, *Regulatory Impact*, *Reputational Impact* and *Third-party Impact*. Moreover, five additional criteria have been included based on expert opinions such as *Health/Safety Impact*, *Employee Impact*, *Customer Impact*, *Speed of Onset* and *Security risk*.

Which key performance indicators are used by organizations in practice and how?

The study has shown that [RTO](#) and [RPO](#) are still the most common KPI's used by organisations and that almost no other measures are used. However, organisations are looking towards new measures to assess and measure their continuity performance better. The KPI's are used primarily as objectives for organisations IT departments without understanding the value gained by achieving those objectives.

Which method should be used by organisations in order to properly assess assets qualitatively and quantitatively while being usable in practice?

Based on the research in this study, a practical method was designed to help organisations approach their continuity assessment in a structured and repeatable manner that allows for different levels of detail and provides long-term goals and changes to the organisation. We also show that taking a process/value-based view of the organisation provides a better and more precise understanding of the actual impact of a disruption. Highlighting that quantifying the problems a disruption can cause is the first step an organisation must take in their continuity management to design cost-effective solutions and satisfy the organisation's risk appetite.

11.2 KEY CONTRIBUTIONS

11.2.1 *Contribution to theory*

Literature in continuity management is often too generalised and contains few directly usable approaches or is highly specialised in one area. The interviewees have noticed the lack of research, but they also expect it to increase significantly soon due to the COVID-19 pandemic and related disruptions. But also a rise in cyber attacks is expected to increase the relevance of continuity management soon. This research is one of the first to provide empirical evidence of used criteria and approaches in continuity management.

Besides the criteria, we have developed a method to assess the critical continuity properties of assets of an organisation, including the criteria as mentioned above and KPI's. This method extends the currently present methods in the literature as well as it could be used to extend the current standards for continuity management like ISO:27031:2011, with more guidelines for organisations. We, therefore, believe that this research contributes significantly to the Continuity management sector.

We have provided a first example for further research by investigating a small group of organisations and highlighting their current approaches, this also provides a more realistic view on the used criteria and processes. Researchers can use this thesis to further improve the assessment of assets in IT continuity management, investigate the actual effectiveness of a more quantified assessment when organisations make use of it.

11.2.2 *Contribution to practice*

On the practical side, this research provides a method for assessing assets for continuity management based on empirical practices to help organisations assess and improve their continuity management systems and approaches. Moreover, the research provides organisations with a concrete set of assessment criteria and KPI's to use in their

continuity management approach aiming for better quantification of the impact of a disruption. A long term goal towards *continuity by design* has been proposed for organisations to improve their continuity capabilities further and turn it into a core requirement in the organisation.

Organisations can use this research to further improve their continuity capabilities, assess the impact of disruptions in the organisation and use the identified stages to create long term goals and strategies for further development. Furthermore, the ability to quantify the potential impact of a disruption also allows the continuity management team to support their arguments for further investment into the continuity capabilities of the organisation.

11.2.3 Findings

Significant findings of this research have been outlined below.

1. There is no one right way for assessing continuity management assets

We have found that most organisations do not follow any standardised approach as proposed in the literature. While there are many common denominators between organisations in approaching continuity management, no standard provides organisations with enough information and guidelines to be implemented widely. The guidelines lack core steps like assessing assets and leave organisations to determine how to assess assets. This leads to vastly different approaches, making the use of a standard pointless. Furthermore, organisations consider different criteria and risks more or less relevant to them. Currently, the best approach in our eyes would be using the method developed in this thesis, in combination with the structured approach of the standard, to create a comparable and repeatable assessment.

2. Quantifying the impact of a disruption is the basis for successful continuity management

Business Continuity management tries to assess the impact of a disruption in an organisation. However, most current approaches do not quantify the impact that the disruption would cause. When considering that organisations are trying to mitigate risks and staying inside their *risk appetite*, only when the organisation can quantify the impact of disruption can they evaluate if they are still inside their risk appetite.

3. Communication is one of the keys for successful continuity management

We found that communication is one of the keys to successful continuity management. Almost all organisations indicated that most present problems in their continuity management could be improved with better communication between the different departments and a shift away from seeing continuity management as a "budget issue". This implies more support and investment from management into continuity management systems and projects.

4. Continuity management should focus on impact

Continuity management should shift from risk-based assessment towards impact-based assessment. This refers to the idea that a risk-based assessment will only cover known risks, leaving the organisation unprepared for unknown disasters. This can be exceptionally seen with the COVID-19 pandemic, which was an unknown risk to most organisations at that time, and they were not prepared for such an event. Focusing on impact would allow organisations to concentrate on the assets and how they can be recovered, or at least the impact is limited regardless of the disruption.

5. Process/Value chain provides a clearer perspective

While some organisations are shifting away from the isolated view on assets in IT and consider the process and value generation that the assets are involved in as the focus of their assessment. Many large organisations still consider IT assets in an isolated state as if they are not a highly integral part to the organisation with many dependencies that could be affected during a disruption. Ultimately it is up to the organisation on what perspective they will take and investigate their assets; however, only when the whole process is considered can the full impact of disruption be evaluated.

11.3 RELATED & FUTURE WORK

During this research, more papers and books have been published in the (IT) Business Continuity Management domain, which has not been included in our literature review or during later research. Our claim for the relevance of our study is therefore limited to the time of the data collection in June 2021. An exploratory literature review has shown that as of February 2022, academic contributions about business continuity and impact assessment include:

- Sergei Petrenko, "Developing an Enterprise Continuity Program," in *Developing an Enterprise Continuity Program*, River Publishers, 2021 [36]

-this book was not accessible but has been selected based on the chapter abstracts

- N. Russo, L. Reis, C. Silveira and H. S. Mamede, "Framework for designing Business Continuity - Multidisciplinary Evaluation of Organizational Maturity," 2021 16th Iberian Conference on Information Systems and Technologies (CISTI), 2021, pp. 1-4 [40]

However, no papers covering the same topic has been found, which shows that the relevance of this study remains.

Moreover, thesis has only studied the continuity management assessment in organisations' IT. In order to design a method that can be applied successfully in other areas where continuity management is of relevance, other organisations must be studied, and more research performed to identify and establish criteria and KPI's for all sectors and industries.

Organisations struggle to include probabilities in the assessment, as it is unclear what disruption would occur and why. It is challenging for organisations to judge how often a disruption impacts certain assets. Future research should investigate how organisations can include risk probabilities for unknown risks on assets, giving them a better understanding of assets at risk.

Another concern that should be investigated is a better inclusion of risk assessment into the method. Currently, most organisations perform a risk-based assessment, including indirect impacts in the assessment. Since we did not investigate how the risks can be used in our impact-based assessment to provide additional value, this is also an area that should be researched in more detail.

Lastly, this study proposed as the last stage for organisations *continuity by design*. Since we have not seen any large organisation being able to implement a *continuity by design* approach, future research should investigate how large organisations can make the shift to *continuity by design* and what else should be entailed in this last step.

11.3.1 Limitations

This research only looked at medium and large organisations in Germany and the Netherlands active in the IT sector, therefore, this limits the findings and generalisations to these organisations and countries.

Moreover, we have only been able to show a demonstration of the method on two examples at Thales. A real implementation and observation of the method and criteria would be necessary and best be used during a real disaster to establish the actual usefulness of the new method.

Part I

APPENDIX

APPENDIX

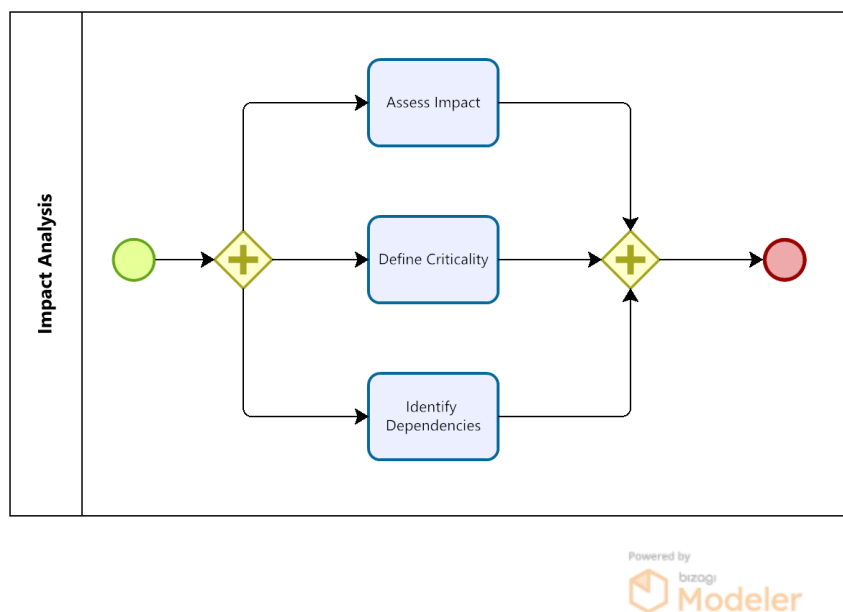


Figure A.1: Impact Analysis

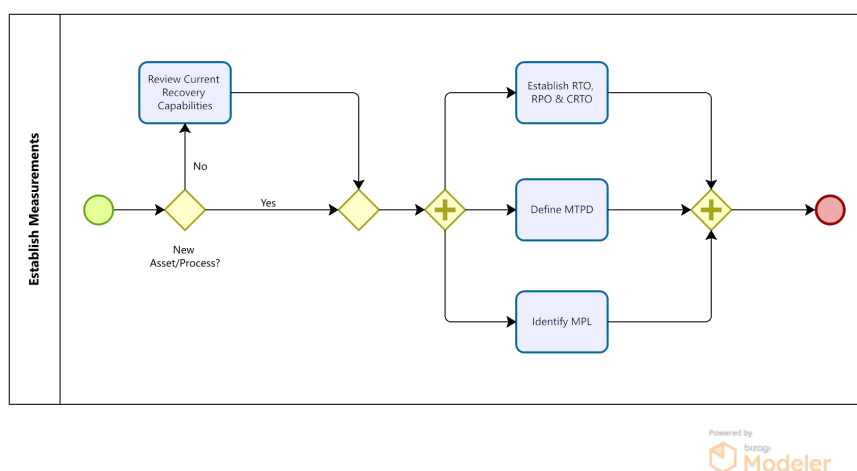


Figure A.2: Key Performance Indicators

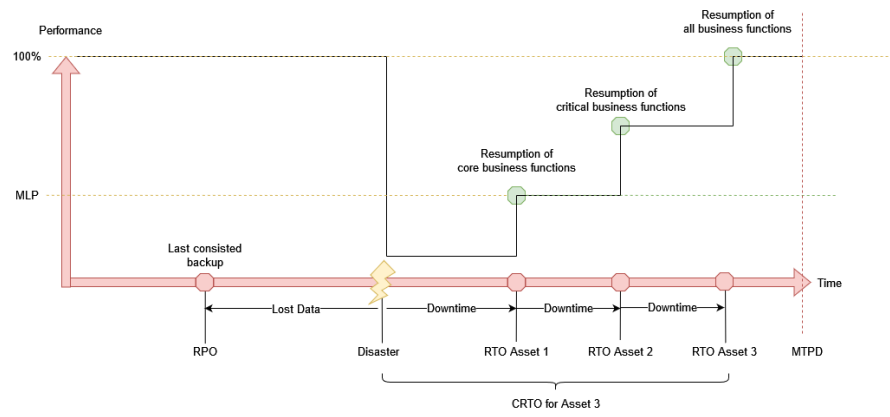


Figure A.3: BCM key performance indicators

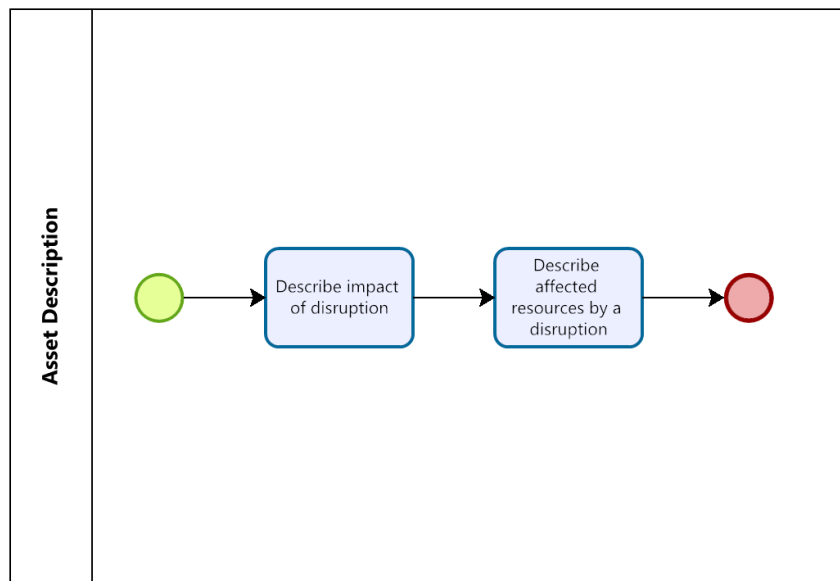


Figure A.4: Assess description steps

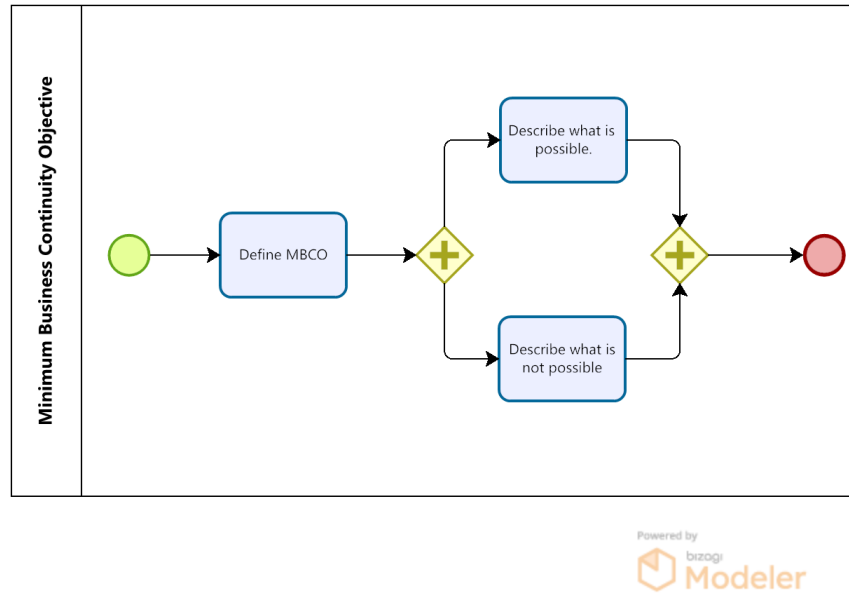


Figure A.5: Emergency Operations Level

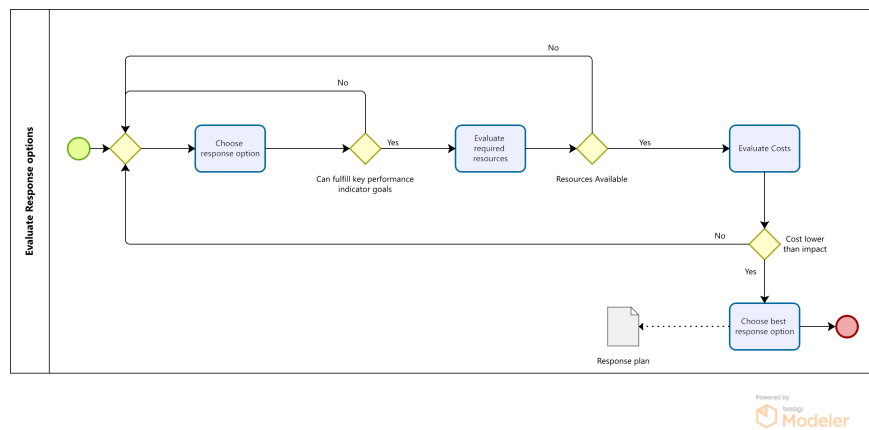


Figure A.6: Response process

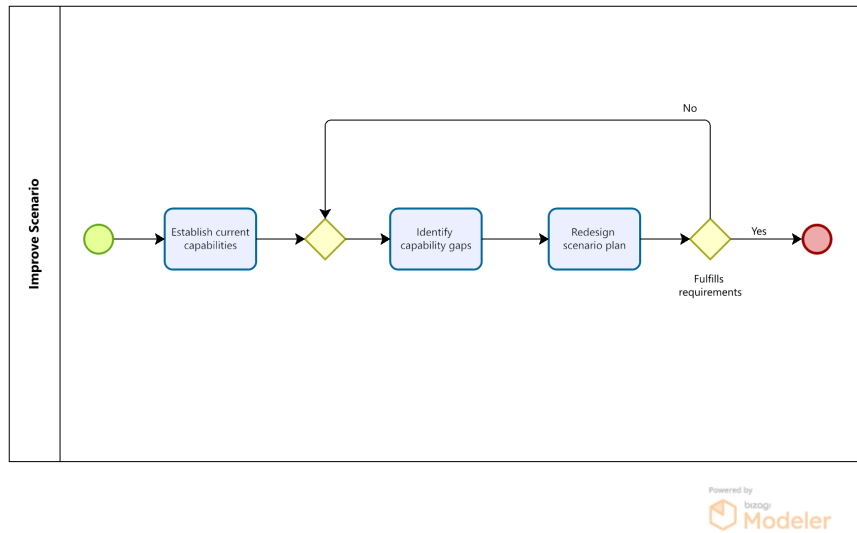


Figure A.7: Improve Scenario process

BIBLIOGRAPHY

- [1] Hevner Alan, R Alan, March Salvatore, T Salvatore, Park, Park Jinsoo, Ram, and Sudha. "Design Science in Information Systems Research." In: *Management Information Systems Quarterly* 28 (Mar. 2004), p. 75.
- [2] O. H. Alhazmi and Y. K. Malaiya. "Evaluating disaster recovery plans using the cloud." In: *2013 Proceedings Annual Reliability and Maintainability Symposium (RAMS)* (2013). DOI: [10.1109/rams.2013.6517700](https://doi.org/10.1109/rams.2013.6517700).
- [3] Omar H. Alhazmi and Yashwant K. Malaiya. "Assessing Disaster Recovery Alternatives: On-Site, Colocation or Cloud." In: *2012 IEEE 23rd International Symposium on Software Reliability Engineering Workshops*. IEEE. DOI: [10.1109/issrew.2012.20](https://doi.org/10.1109/issrew.2012.20).
- [4] Angraini et al. "Risk Assessment on Information Asset an academic Application Using ISO 27001." In: *2018 6th International Conference on Cyber and IT Service Management (CITSM)*, pp. 1–4. DOI: [10.1109/CITSM.2018.8674294](https://doi.org/10.1109/CITSM.2018.8674294). URL: <https://ieeexplore.ieee.org/document/8674294/>.
- [5] Julian Araujo, Paulo Maciel, Ermeson Andrade, Gustavo Calou, Vandi Alves, and Paulo Cunha. "Decision making in cloud environments: an approach based on multiple-criteria decision analysis and stochastic models." In: *Journal of Cloud Computing* 7.1 (2018). ISSN: 2192-113X. DOI: [10.1186/s13677-018-0106-7](https://doi.org/10.1186/s13677-018-0106-7). URL: <https://journalofcloudcomputing.springeropen.com/track/pdf/10.1186/s13677-018-0106-7>.
- [6] Y. P. Baginda, A. Affandi, and I. Pratomo. "Analysis of RTO and RPO of a Service Stored on Amazon Web Service (AWS) and Google Cloud Engine (GCE)." In: *2018 10th International Conference on Information Technology and Electrical Engineering (ICITEE)*, pp. 418–422. DOI: [10.1109/ICITEED.2018.8534758](https://doi.org/10.1109/ICITEED.2018.8534758). URL: <https://ieeexplore.ieee.org/document/8534758/>.
- [7] Dr Lim Yew Ban. *What Is MBCO or Minimum Business Continuity Objective?* Sept. 2018. URL: <https://blog.bcm-institute.org/bcm-planning-methodology/what-is-mbco-or-minimum-business-continuity-objective>.
- [8] Pearl Brereton, Barbara A. Kitchenham, David Budgen, Mark Turner, and Mohamed Khalil. "Lessons from applying the systematic literature review process within the software engineering domain." In: *Journal of Systems and Software* 80.4 (2007), 571–583. DOI: [10.1016/j.jss.2006.07.009](https://doi.org/10.1016/j.jss.2006.07.009).

- [9] Sharon L. Burton. "Protection Via Business Impact Analysis in a Cyber World: A 3-Part Series." In: *Advances in Intelligent Systems and Computing 17th International Conference on Information Technology–New Generations (ITNG 2020)* (May 2020), 3–8. DOI: [10.1007/978-3-030-43020-7_1](https://doi.org/10.1007/978-3-030-43020-7_1).
- [10] Virginia Cerullo and Michael J. Cerullo. "Business Continuity Planning: A Comprehensive Approach." In: *Information Systems Management* 21.3 (2004), pp. 70–78. ISSN: 1058-0530. DOI: [10.1201/1078/44432.21.3.20040601/82480.11](https://doi.org/10.1201/1078/44432.21.3.20040601/82480.11).
- [11] Gang Chen. "Improvement Model of Business Continuity Management on E-Learning." In: *Advances in Computer Science and Education*. Springer Berlin Heidelberg, 2012, pp. 1–5. ISBN: 1867-5662. DOI: [10.1007/978-3-642-27945-4_1](https://doi.org/10.1007/978-3-642-27945-4_1).
- [12] "Contingency and continua: achieving excellence through business continuity planning." In: *Business Horizons* 40.6 (1997), pp. 19–25. ISSN: 0007-6813. DOI: [10.1016/S0007-6813\(97\)90063-X](https://doi.org/10.1016/S0007-6813(97)90063-X).
- [13] Adrian Davis. "What Is Critical to Your Infrastructure?" In: *Infosecurity* 8.5 (2011), pp. 18–21. ISSN: 1754-4548. DOI: [10.1016/S1754-4548\(11\)70064-X](https://doi.org/10.1016/S1754-4548(11)70064-X).
- [14] Daniel Dimase et al. "Systems engineering framework for cyber physical security and resilience." In: *Environment Systems and Decisions* 35.2 (2015), pp. 291–300. ISSN: 2194-5403. DOI: [10.1007/s10669-015-9540-y](https://doi.org/10.1007/s10669-015-9540-y).
- [15] Mariana Gerber and Rossouw Von Solms. "Management of risk in the information age." In: *Computers & Security* 24.1 (2005), pp. 16–30. ISSN: 0167-4048. DOI: [10.1016/j.cose.2004.11.002](https://doi.org/10.1016/j.cose.2004.11.002).
- [16] Michael Gibbert, Winfried Ruigrok, and Barbara Wicki. "What Passes as a Rigorous Case Study?" In: *Strategic Management Journal* 29.13 (2008), pp. 1465–1474. ISSN: 01432095, 10970266. URL: <http://www.jstor.org/stable/40060241>.
- [17] Mel Gosling. *Maximum Tolerable Period of disruption: a New Definition*. Jan. 2011. URL: <https://continuitycentral.com/feature0845.html>.
- [18] Viral Gupta et al. "Exploring disaster recovery parameters in an enterprise application." In: *2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)* (2016). DOI: [10.1109/iciccs.2016.7542345](https://doi.org/10.1109/iciccs.2016.7542345).
- [19] Brahim Herbane. "The evolution of business continuity management: A historical review of practices and drivers." In: *Business History* 52.6 (2010), 978–1002. DOI: [10.1080/00076791.2010.511185](https://doi.org/10.1080/00076791.2010.511185).
- [20] Deborah Higgins and Business Continuity Institute. *Good Practice Guidelines : the Global Guide to Good Practice in Business Continuity*. The Business Continuity Institute, 2017. ISBN: 9780993211089.

- [21] Leong Lai Hoong and Govindan Marthandan. "Factors influencing the success of the disaster recovery planning process: A conceptual paper." In: *2011 International Conference on Research and Innovation in Information Systems*. IEEE. DOI: [10.1109/icriis.2011.6125683](https://doi.org/10.1109/icriis.2011.6125683).
- [22] Y. Huanchun. "A Study on the Risk Hierarchical Model and Risk Conduction Based on the Enterprise Complex Information System." In: *2009 International Forum on Information Technology and Applications*. Vol. 3, pp. 595–599. DOI: [10.1109/IFITA.2009.298](https://doi.org/10.1109/IFITA.2009.298). URL: <https://ieeexplore.ieee.org/document/5232196/>.
- [23] ISO 22301:2012. June 2012. URL: <https://www.iso.org/standard/50038.html>.
- [24] ISO 22301:2019. Sept. 2019. URL: <https://www.iso.org/standard/75106.html>.
- [25] ISO 27031:2011. Mar. 2011. URL: <https://www.iso.org/standard/44374.html>.
- [26] Peter Katsumata et al. "Cybersecurity risk management." In: *2010 - MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE*. IEEE. DOI: [10.1109/milcom.2010.5680181](https://doi.org/10.1109/milcom.2010.5680181).
- [27] Gregory King. *Oracle VM 3: Overview of Disaster Recovery Solutions*. May 2015. URL: https://informationsecurity.report/Resources/Whitepapers/20228f7e-20f0-47a3-a729-02b0083eadd2_Oracle\%20VM\%203\%20overview.pdf.
- [28] Barbara Kitchenham and Pearl Brereton. "A systematic review of systematic review process research in software engineering." In: *Information and Software Technology* 55.12 (2013), 2049–2075. DOI: [10.1016/j.infsof.2013.07.010](https://doi.org/10.1016/j.infsof.2013.07.010).
- [29] P. Kokkinos et al. "Survey: Live Migration and Disaster Recovery over Long-Distance Networks." In: *ACM Computing Surveys* 49 (July 2016), pp. 1–36. DOI: [10.1145/2940295](https://doi.org/10.1145/2940295).
- [30] Difana Meilani et al. "Designing Disaster Recovery Plan of Data System for University." In: *IOP Conference Series: Materials Science and Engineering* 697 (2019), p. 012028. DOI: [10.1088/1757-899x/697/1/012028](https://doi.org/10.1088/1757-899x/697/1/012028).
- [31] J. Mendonça et al. "Multiple-criteria Evaluation of Disaster Recovery Strategies Based on Stochastic Models." In: *2020 16th International Conference on the Design of Reliable Communication Networks DRCN 2020*, pp. 1–7. DOI: [10.1109/DRCN48652.2020.1570614925](https://doi.org/10.1109/DRCN48652.2020.1570614925). URL: <https://ieeexplore.ieee.org/document/9089342/>.
- [32] Hossam Abdel Rahman Mohamed. "A Proposed Model for IT Disaster Recovery Plan." In: *International Journal of Modern Education and Computer Science* 6.4 (2014), 57–67. DOI: [10.5815/ijmeecs.2014.04.08](https://doi.org/10.5815/ijmeecs.2014.04.08).

- [33] Jeffrey Mounzer et al. "Integrated security risk management for IT-intensive organizations." In: *2010 Sixth International Conference on Information Assurance and Security*. IEEE. DOI: [10.1109/isias.2010.5604086](#).
- [34] Cyril Onwubiko and Karim Ouazzane. "SOTER: a Playbook for Cybersecurity Incident Management." In: *IEEE Transactions on Engineering Management* (2020), 1–21. DOI: [10.1109/TEM.2020.2979832](#). URL: <https://ieeexplore.ieee.org/abstract/document/9086465/>.
- [35] C. A. Peterson. "Business Continuity Management & guidelines." In: pp. 114–120. ISBN: 9781605586618 (ISBN). DOI: [10.1145/1940976.1940999](#).
- [36] Sergei Petrenko. "Developing an Enterprise Continuity Program." In: *Developing an Enterprise Continuity Program*. 2021, pp. i–lxx.
- [37] Athanasios Podaras. "A Non-arbitrary Method for Estimating IT Business Function Recovery Complexity via Software Complexity." In: *Lecture Notes in Business Information Processing*. Springer International Publishing, 2015, pp. 144–159. ISBN: 1865-1348. DOI: [10.1007/978-3-319-19297-0_10](#).
- [38] Carmen Păunescu and Ruxandra Argatu. "CRITICAL FUNCTIONS IN ENSURING EFFECTIVE BUSINESS CONTINUITY MANAGEMENT. EVIDENCE FROM ROMANIAN COMPANIES." In: *Journal of Business Economics and Management* 21.2 (2020), pp. 497–520. ISSN: 1611-1699. DOI: [10.3846/jbem.2020.12205](#). URL: <https://journals.vgtu.lt/index.php/JBEM/article/download/12205/9836>.
- [39] M. Rabbani et al. "Developing a two-step fuzzy cost–benefit analysis for strategies to continuity management and disaster recovery." In: *Safety Science* 85 (2016), pp. 9–22. ISSN: 0925-7535. DOI: [10.1016/j.ssci.2015.12.025](#).
- [40] Nelson Russo, Leonilde Reis, Clara Silveira, and Henrique São Mamede. "Framework for designing Business Continuity - Multidisciplinary Evaluation of Organizational Maturity." In: *2021 16th Iberian Conference on Information Systems and Technologies (CISTI)*. 2021, pp. 1–4. DOI: [10.23919/CISTI52073.2021.9476297](#).
- [41] N. Sahebjamnia et al. "Integrated business continuity and disaster recovery planning: Towards organizational resilience." In: *European Journal of Operational Research* 242.1 (2015), pp. 261–273. ISSN: 03772217. DOI: [10.1016/j.ejor.2014.09.055](#).
- [42] Priti Sikdar. "Alternate Approaches to Business Impact Analysis." In: *Information Security Journal: A Global Perspective* 20.3 (2011), 128–134. DOI: [10.1080/19393555.2010.551274](#).

- [43] S. Ali Torabi et al. "An enhanced risk assessment framework for business continuity management systems." In: *Safety Science* 89 (2016), pp. 201–218. ISSN: 09257535. DOI: [10.1016/j.ssci.2016.06.015](https://doi.org/10.1016/j.ssci.2016.06.015).
- [44] John Venable, Jan Pries-Heje, and Richard Baskerville. "FEDS: a Framework for Evaluation in Design Science Research." In: *European Journal of Information Systems* 25.1 (2016), pp. 77–89. ISSN: 0960-085X. DOI: [10.1057/ejis.2014.36](https://doi.org/10.1057/ejis.2014.36). URL: <https://doi.org/10.1057/ejis.2014.36>.
- [45] Montri Wiboonrat. "An empirical IT contingency planning model for disaster recovery strategy selection." In: *2008 IEEE International Engineering Management Conference*. IEEE. DOI: [10.1109/iemce.2008.4617953](https://doi.org/10.1109/iemce.2008.4617953).
- [46] Roel J. Wieringa. *Design Science Methodology for Information Systems and Software Engineering*. Springer Berlin Heidelberg, 2014.
- [47] Robert K. Yin. *Case Study Research and Applications: Design and Methods*. 6th ed. SAGE Publications, Sept. 2017. ISBN: 9781506336169.
- [48] H. Zare et al. "Business Continuity Plan and Risk Assessment Analysis in Case of a Cyber Attack Disaster in Healthcare Organizations." In: ed. by S. Latifi. Vol. 1134. Springer, 2020, pp. 137–144. ISBN: 21945357 (ISSN); 9783030430191 (ISBN). DOI: [10.1007/978-3-030-43020-7_19](https://doi.org/10.1007/978-3-030-43020-7_19).
- [49] *enterprise risk management - integrated framework*. Coso, 2004.
- [50] *how pulse connect secure works*. URL: https://docs.pulsesecure.net/WebHelp/PCS/8.3R3/Content/PCS/PCS_AdminGuide_8.3/How_Pulse_Connect_Secure_Works.htm.
- [51] *pcb manufacturing process & equipment - pcbway*. URL: <https://www.pcbway.com/pcb-service.html>.

COLOPHON

This document was typeset using the typographical look-and-feel classicthesis developed by André Miede. The style was inspired by Robert Bringhurst's seminal book on typography "*The Elements of Typographic Style*". classicthesis is available for both L^AT_EX and L^YX:

<https://bitbucket.org/amiede/classicthesis/>

Happy users of classicthesis usually send a real postcard to the author, a collection of postcards received so far is featured here:

<http://postcards.miede.de/>

Final Version as of April 23, 2022 (classicthesis).