



UNIVERSITY  
OF TWENTE.

# *Aligning Information Systems Management and Risk Management to achieve Enterprise Resilience*

---

Master's Thesis, Business Information Technology

Jasper van Loevezijn – University of Twente

Enschede, Netherlands, 4-7-2023

**Supervisors:**

Dr. ir. Marten van Sinderen, University of Twente, Faculty of EEMCS

Dr. Renata Guizzardi – Silva Souza, University of Twente, Faculty of BMS

Rebecca Hulleman, Senior Consultant IT assurance at KPMG NL



# Executive summary

---

In today's highly competitive global business environment, the need for **Enterprise Resilience** has become paramount. Enterprises must anticipate and prepare for disruptions while effectively recovering, adapting, and learning from them. However, many companies lack practical resources to build resilience, despite the growing interest in the field. This research aims to bridge this gap by designing and validating a method that **aligns Information Systems Management** and **Risk Management** to enhance **Enterprise Resilience**. By leveraging key aspects from both fields, this method offers a practical framework for organizations to strengthen their resilience and gain a sustainable competitive advantage. Through a comprehensive review of existing literature, insights from industry experts, and validation, this research seeks to contribute to the practical advancement of Enterprise Resilience and its crucial role in navigating today's turbulent and interconnected risk landscape.

**Key findings:** This thesis outlines the development and validation of the novel **Enterprise Resilience enhancement method** (*Chapter 6*). By aligning and harmonizing activities from Information Systems Management and Risk Management, the method offers organizations a **structured** and **practical** approach to significantly bolster their Enterprise Resilience, through essential aspects of modern organizations. The method's development has been shaped through rigorous design and validation phases, drawing from existing literature and engaging with practitioners in the respective fields. The ER enhancement method consists of a visual representation and an accompanying maturity tracker, facilitating its practical adoption and enabling organizations to track their progress in enhancing Enterprise Resilience. It emphasizes the importance of a **resilience-aware culture** within organizations for achieving high maturity in Enterprise Resilience. The comprehensive development process can be retraced as described in *Chapter 5*, the development was executed according to the pre-specified requirements and methodological considerations presented in *Chapter 4*.

**Methodologies:** The **Design Science Methodology** by Wieringa (2014) is selected as the primary design methodology, supplemented by additional methodologies for data collection at different stages of the design process. A **systematic literature review**, following the methodology proposed by Kitchenham and Charters (2007), establishes the research foundation (*Chapter 3*). The Design Science Methodology, characterized by iterative problem-solving and answering of knowledge questions, guides the design cycle comprising the phases of problem investigation, treatment design, and treatment validation. The iterative design process is supported by gathering novel insights and feedback from expert practitioners through **semi-structured interviews**. The concluding iteration of the ER enhancement method is validated through **case studies**, simulating true implementation. A comprehensive description of the used methodologies is presented in *Chapter 2*.

**Validation:** The final iteration of the ER enhancement method was validated using two instruments. The method's adherence to pre-specified **functional** and **non-functional requirements** was confirmed. Furthermore, **case studies** simulated the method's implementation in different environments, all resulting in positive outcomes. Measured changes in the level of Enterprise Resilience showed significant improvement across key abilities essential to fostering Enterprise Resilience. The method offered benefits such as fostering a **resilient-aware culture**, emphasizing **proactive solutions**, and documenting

**response plans.** Its **continuous and iterative nature** was also recognized as advantageous for promoting resilience throughout the organization. The validation efforts are documented in *Chapter 7*.

**Keywords:** *Enterprise Resilience, Information Systems Management, Risk Management, Method, Maturity Model, Case Study*

# Acknowledgements

---

I would like to express my sincere gratitude to my supervisor, Rebecca Hulleman, for her guidance and support throughout the duration of this thesis. I very much enjoyed working together and I believe our collaboration has led to a very respectable product as a result of my thesis. I am also grateful to KPMG for granting me the opportunity to conduct my research in collaboration with their organization, giving me access to an extensive and valuable network of knowledge and expertise.

Additionally, I would like to express my gratitude to my supervisors, Marten van Sinderen and Renata Guizzardi – Silva Souza, from the University of Twente. Their profound expertise and invaluable guidance in the realm of academic research have been instrumental in my growth and development. I am deeply appreciative of the valuable lessons I have learned under their supervision.

I would also like to acknowledge and thank all the experts who have contributed their time, knowledge, and expertise to this research. Their valuable insights and perspectives have added significant value to the study and have helped broaden my understanding of the subject matter.

# Table of contents

Executive summary .....	i
Acknowledgements .....	iii
Table of contents.....	iv
List of Figures.....	viii
List of Tables.....	ix
List of Abbreviations .....	x
1 Introduction .....	1
1.1 Problem Statement & Research Objective .....	1
1.2 Research Scope.....	2
1.3 Stakeholder analysis .....	3
1.4 Research questions.....	5
1.5 Thesis structure.....	8
2 Research design .....	9
2.1 Design science methodology.....	9
2.1.1 Design problem.....	10
2.1.2 Design plan .....	12
2.1.3 Design cycles.....	13
2.2 Research methodologies.....	14
2.2.1 Systematic literature review.....	14
2.2.2 Interview.....	15
2.2.3 Case study .....	16
2.3 Summary.....	16
3 Literature review.....	18
3.1 SLR Methodology.....	18
3.1.1 Planning the review .....	18
3.1.2 Conducting the review.....	19
3.1.2.1 Literature database selection .....	19
3.1.2.2 Search query formulation .....	19
3.1.2.3 Selection criteria.....	20
3.1.2.4 Article selection .....	20
3.2 Definitions .....	22
3.2.1 Enterprise Resilience .....	23
3.2.1.1 Enterprise Resilience qualities .....	24

---

3.2.1.2	Disruptions .....	27
3.2.1.3	Definition .....	28
3.2.2	Information Systems Management .....	28
3.2.2.1	Definition .....	30
3.2.3	Risk Management .....	30
3.2.3.1	Risk Management strategies .....	31
3.2.3.2	Definition .....	32
3.3	Information Systems Management & Enterprise Resilience .....	32
3.4	Risk Management & Enterprise Resilience .....	35
3.5	Discussion .....	38
4	Requirements Analysis & Methodological Considerations .....	40
4.1	Requirements .....	40
4.1.1	Functional requirements .....	41
4.1.2	Non-functional requirements .....	42
4.2	Design Approach .....	44
4.2.1	Design of initial artefact .....	45
4.2.2	Design choices and method dimensions .....	48
4.2.3	ArchiMate .....	49
4.3	Validation approach .....	51
4.3.1	Gathering expert opinion through semi-structured interviews .....	51
4.3.2	Apply the method in a case study .....	52
4.4	Summary .....	53
5	Development .....	55
5.1	Cycle 1 .....	55
5.1.1	Design: The initial artefact .....	55
5.1.2	Validation: Interviews & Requirement satisfaction .....	59
5.1.2.1	Expert opinion through interviews .....	59
5.1.2.2	Requirement satisfaction .....	62
5.2	Cycle 2 .....	63
5.2.1	Design .....	63
5.2.2	Validation: Interviews & Requirement satisfaction .....	65
5.2.2.1	Expert opinion through interviews .....	65
5.2.2.2	Requirement satisfaction .....	67
5.3	Summary .....	68
6	ER Enhancement Method .....	70
6.1	Final design considerations .....	70

---

6.2	Finalized method.....	71
7	Validation .....	75
7.1	Case study .....	75
7.1.1	Case 1: Potential leak at financial services firm.....	76
7.1.1.1	Case description: Citrix leak .....	76
7.1.1.2	Case 1: Results.....	76
7.1.1.3	Case 1: Observations.....	78
7.1.1.4	Case 1: Concluding remarks .....	79
7.1.2	Case 2: System outage at a retail chain store .....	80
7.1.2.1	Case description: Warehouse management system outage.....	80
7.1.2.2	Case 2: Results.....	80
7.1.2.3	Case 2: Observations.....	81
7.1.2.4	Case 2: Concluding remarks .....	83
7.2	Requirement satisfaction.....	83
7.3	Validation conclusion.....	86
8	Discussion.....	88
8.1	Reflection on methodology .....	88
8.1.1	Design Science Methodology .....	88
8.1.2	Semi-structured interviews .....	88
8.1.3	Case study .....	89
8.2	Reflection on ER enhancement method .....	90
8.3	Limitations.....	90
9	Conclusion .....	92
9.1	Summary & Main Conclusions .....	92
9.1.1	Sub-Research Questions .....	92
9.1.2	Primary Research Question .....	96
9.2	Contributions.....	97
9.2.1	Contributions to Science .....	97
9.2.2	Contributions to Practice .....	98
9.3	Future work .....	98
10	Bibliography.....	100
11	Appendix.....	104
	Appendix A: Desired interviewee profiles.....	104
	Appendix B: Interview Questions .....	105
	Appendix C: Case description (Example: COVID-19).....	107
	Appendix D: Case study questions .....	109



Appendix E: Method after treatment design cycle 2 (ER enhancement method, cycle 2)	112
Appendix F: Maturity Matrix continuous monitoring & auditing at Consulting firm.....	114
Appendix G: Maturity tracker (Excel).....	115
Appendix H: Case study 1, maturity tracker results (Participant 3.1) .....	120
Appendix I: Case study 2, maturity tracker results (Participant 3.2).....	122

---

# List of Figures

---

Figure 1: Stakeholders, drivers, and goals for increasing Enterprise Resilience .....	4
Figure 2: Engineering cycle (Wieringa, 2014) .....	10
Figure 3: Research process mapped on the design cycle by Wieringa (2014) .....	12
Figure 4: Screening process RQ1.1 & RQ1.2 .....	21
Figure 5: Balanced resilience (Pettit et al., 2010).....	24
Figure 6: Disruption pattern (Madani & Parast, 2023) .....	28
Figure 7: DeLone & McLean model of IS success (DeLone & McLean, 1992).....	29
Figure 8: Updated DeLone & McLean model of IS success (DeLone & McLean, 2003).....	29
Figure 9: Conceptual diagram of IS (Mallach, 2015) .....	30
Figure 10: Risk matrix (Ni et al., 2010) .....	32
Figure 11: Appropriate strategies for different operating conditions (Pettit et al., 2014) .....	36
Figure 12: Business layer, application layer, and technology layer of ArchiMate (The Open Group, 2023) .....	50
Figure 13: ArchiMate business layer elements (The Open Group, 2023).....	50
Figure 14: ArchiMate application layer elements (The Open Group, 2023).....	50
Figure 15: ArchiMate technology layer elements, and value stream element (The Open Group, 2023) .....	51
Figure 16: ArchiMate relationships: realization relationship, triggering relationship, composition relationship (The Open Group, 2023) .....	51
Figure 17: Initial design based on literature findings (ER enhancement method, cycle 1).....	58
Figure 18: Addition of people and collaborations to the ER enhancement method .....	64
Figure 19: ER enhancement method, final edition .....	74

# List of Tables

Table 1: Design cycle activities.....	14
Table 2: Seven steps to conducting, analysing, and reporting semi-structured interview data (Adeoye-Olatunde & Olenik, 2021).....	15
Table 3: Scientific databases.....	19
Table 4: Selection criteria.....	20
Table 5: RQ1.1 article selection.....	21
Table 6: RQ1.2 article selection.....	22
Table 7: ER qualities.....	25
Table 8: Main findings RQ1.1.....	34
Table 9: Main findings RQ1.2.....	37
Table 10: List of functional requirements.....	41
Table 11: List of non-functional requirements.....	42
Table 12: List of non-functional requirements and indicators.....	44
Table 13: Risk Management aspects leading to ER.....	45
Table 14: Information Systems Management aspects leading to ER.....	47
Table 15: Design cycle activities.....	55
Table 16: First-round interviewees' data.....	59
Table 17: Main findings from the first round of interviews.....	60
Table 18: Second round interviewees' data.....	65
Table 19: Main findings from the second round of interviews.....	65
Table 20: Case study participants.....	75
Table 21: Baseline level of ER case study 1 (Hollnagel, 2010).....	77
Table 22: ER enhancement method; maturity tracker average results case study 1.....	77
Table 23: Resulting level of ER case study 1, using Hollnagel (2010).....	77
Table 24: Baseline level of ER case study 2 (Hollnagel, 2010).....	80
Table 25: ER enhancement method; maturity tracker average results case study 2.....	81
Table 26: Resulting level of ER case study 2, using Hollnagel (2010).....	81
Table 27: Functional requirements implementation justification.....	84
Table 28: Non-functional requirements implementation justification.....	85

---

# List of Abbreviations

---

<b><i>Abbreviation</i></b>	<b>Definition</b>
<i>AI</i>	Artificial intelligence
<i>BCM</i>	Business continuity management
<i>EA</i>	Enterprise architecture
<i>ER</i>	Enterprise resilience
<i>ERM</i>	Enterprise risk management
<i>ERP</i>	Enterprise resource planning
<i>IS</i>	Information system
<i>IT</i>	Information technology
<i>MIS</i>	Management information system
<i>SLR</i>	Systematic literature review

---

# 1 Introduction

---

This chapter serves to introduce and motivate the undertaken research. It begins by outlining the contextual background of the problem and subsequently delineates the primary objective of the study. In order to formulate a path towards achieving the primary objective, a stakeholder analysis is conducted to identify the areas where this research can generate value. This analysis consequently culminates in the formulation of the primary research question, accompanied by the identification of sub-questions that steer the research process towards attaining the main objective.

I conducted this research during my internship with KPMG in the IT assurance department. KPMG is a multinational professional services network specializing in financial auditing, tax services, and advisory. The IT assurance department possesses comprehensive expertise regarding IT processes, IT systems, IT control frameworks, IT risks, and control measures to mitigate these risks. It consists of a team of consultants that advise client firms on the control, design, governance, and security of IT as well as advising them on how they can manage and remediate IT-related risks and improve the quality of IT systems.

Undertaking this research at KPMG granted me access to an extensive network of experts spanning diverse industries, backgrounds, and global regions. This facilitated the gathering of insights from highly regarded professionals, enriching the research process with a broad range of perspectives. Additionally, I could rely on the knowledge and expertise of IT and risk from everyone in the IT assurance department.

## 1.1 Problem Statement & Research Objective

Enterprise resilience in current days is continuously recognized as a capacity that companies desire to possess. Enterprise resilience can be defined as the capacity of an enterprise to **anticipate, and be prepared for disruption**, as well as the **ability to continuously recover, adapt, and learn from such a disruption** (Hepfer & Lawrence, 2022; Sanchis, Canetta, & Poler, 2020; D. Wang & Chen, 2022). From a strategic perspective, companies have an increased need for strategies to identify the key internal characteristics and external influences which make them susceptible to the impact of foreseen and unforeseen events, due to today's highly competitive global business environment (Hamel & Valikangas, 2004). However, as became apparent from for example the COVID-19 pandemic, enterprises are often not adequately prepared for events of disruptive nature (N. Wang, Cui, & Jin, 2023). This implies a **lack of resources available** in practice that aim to build Enterprise Resilience. The number of studies concerning Enterprise Resilience is growing, this includes studies focusing on the design of resources for increasing Enterprise Resilience that apply to different industries and enterprise sizes (GRC 20/20 Research, 2022; Madni & Jackson, 2009; Sanchis et al., 2020; To & Teer, 2020). Additionally, the International Organization for Standardization released ISO22316:2017, partly focusing on organizational resilience enhancement (International Organization for Standardization, 2017). However, still, only a small number of resources are available that practically enhance Enterprise Resilience, no conceptual approach has received much attention and is accepted by most researchers (Sanchis et al., 2020). But the **need for Enterprise Resilience is present**, since it leads to increased levels of crisis management, and can even become a source of sustainable, competitive advantage and success for

enterprises in a turbulent and changing risk environment (D. Wang & Chen, 2022). And many enterprises find themselves in such an environment these days due to increased globalization, technological complexity, and an increased number of interdependencies (Rohmeyer & Zvi, 2009).

In an attempt to contribute to filling this gap in approaches for enhancing Enterprise Resilience, this research consists of the ***design and validation of a practical method aiming at increasing Enterprise Resilience***. There is no single aspect of an enterprise that individually leads to Enterprise Resilience, working on a single aspect is insufficient to safeguard an organization's resilience (International Organization for Standardization, 2017). Therefore, multiple aspects of an organization must be transformed to ensure practical advancement in terms of Enterprise Resilience, this research proposes the use of ***Risk Management and Information Systems Management***.

Risk Management is concerned with identifying, evaluating, and prioritizing risk followed by the application of resources to minimize, monitor, and control the effects of risks (Hubbard, 2020; International Organization for Standardization, 2018). This makes it a suitable aspect for a company to contribute to the improvement of Enterprise Resilience since Risk Management ***attempts to proactively reduce chances of disruption***. Proactive preparation for disruption is a major part of Enterprise Resilience (Sin & Ng, 2013).

Information Systems Management is the usage of people and information technology and their relationships, for decision-making, coordination, and control within an organization. (Mallach, 2015). Information Systems Management can lead to increased efficiency of communication, and improved data consistency, exchange, and access (Alawamleh, Alshibly, Tommalieh, Al-Qaryouti, & Ali, 2021). However, it also introduces ***increased complexity*** and a ***greater number of dependencies***. And due to the steep increase in end-user computing in businesses, the importance of information systems cannot be ignored. Every business relies on information systems, and therefore an attempt must be made to incorporate Information Systems Management as a contributor to increased Enterprise Resilience. Besides ***leveraging Information Systems Management*** for resilience building, a ***re-examination of information systems usage*** in firms can also be explored as a source of increased Enterprise Resilience. Since aspects like e.g. power or network outages of systems can be a great source of disruption.

The lack of practically applicable methods for improving Enterprise Resilience needs to be reduced, therefore, this research attempts to contribute to filling this gap by designing and validating a method that aligns and harmonizes Information Systems Management and Risk Management with the goal of increasing the level of Enterprise Resilience. The method aims at aligning aspects and activities from Risk Management and Information Systems Management, and provides instructions on how their harmonization can practically be exhausted by firms to enhance their Enterprise Resilience. To design this model, knowledge from existing literature is used, as well as knowledge from practitioners from the fields of Information Systems Management and Risk Management.

## 1.2 Research Scope

Since Enterprise Resilience (ER) is a capacity that is impacted by the entire firm, this research focuses on designing a method that can be implemented at the ***strategic level***. At the strategic level, the long-term strategy of the entire business is conceptualized. Since building ER is a

continuous, long-term process (Erol, Sauser, & Mansouri, 2010), a method that affects it, must be implemented at the strategic level. Decisions at the strategic level affect processes at the operational level down the line. At the operational level, the focus is on the day-to-day running of an operation. But defining all processes on the operational level is outside the scope of this research. This is due to the large number of total operations that would have to be described. Changes at the strategic level might still indirectly impact the operational level down the line.

However, the method does **not serve as a complete overhaul of the current strategy** and does not aim to force a change to current operations. Instead, the method must fit on top of this, to introduce a focus on resilience building into the current strategy, since few companies at the moment have a dedicated plan when it comes to building ER. For a firm to effectively adopt the method, the operation must not be massively disturbed in the process. The goal, therefore, is to design a method that can be adopted by a company without introducing major disruptions. A strategy that can achieve this, is **overlayment**. Overlayment is an adoption mechanism to bring a process framework into an organization without significant changes to the underlying organizational structure (APQC, 2011). Overlayment is fitting to the goal of this research because the method must fit on top of the current operation. Also, to achieve successful adoption, it cannot introduce major disruptions. Therefore, the method recommends the user to review the current strategy, adapt it, and append to it through a resilience-building lens, but modification is not a requirement for adoption.

The resulting method is aimed at companies facing **different risk environments**. Meaning that companies in certain industries are far more susceptible to experiencing disruptions than others, nevertheless, the goal is to design a method that applies to both sides of the spectrum. However, generally speaking, companies that face more aggressive risk environments are often inherently more mature in terms of ER. Therefore, the resulting artefact may in fact be more applicable to companies facing a less aggressive risk environment.

Furthermore, the design of the method does **not revolve around a single sector**. The need for increased ER is found across all sectors because the risk environments of most companies are becoming increasingly volatile and complex (Schinagl, Shahim, Khapova, & Van Den Hooff, 2023). Therefore, the aim is to make the artefact applicable to companies across all sectors.

## 1.3 Stakeholder analysis

The goal of designing a method should be to **improve the situation of stakeholders**. Therefore, the stakeholders dictate the goals and constraints of the design process. This section describes the stakeholders that interact with the to-be-designed method as a result of this research. The connections and interdependencies between stakeholders are shown using the ArchiMate modelling language, specifically its motivation elements, which are used to model stakeholder motivations and reasons (The Open Group, 2023).

The stakeholders directly involved with the artefact can be divided into two groups, those affiliated with a **consulting firm** (KPMG), and those affiliated with the **client firm**. From the consulting firm, these are the IT assurance department, and the consultants operating inside this department. The IT assurance department has a wide knowledge of IT processes, IT systems, IT control frameworks, IT risks, and control measures to mitigate these risks. It consists of a team of consultants that advise client firms on the control, design, governance, and security of IT as well as advising them on how they can manage and remediate IT-related

risks and improve the quality of IT systems. Furthermore, they are concerned with evaluating the design and effectiveness of technology controls and they assess the reliability and security of IT systems and controls.

From the client firm, the stakeholders are the persons or departments responsible for **strategic management**, the persons or departments responsible for **Risk Management**, and the persons or departments responsible for **IT management**. The involved stakeholders and their goals can be seen in Figure 1. It shows what achieving the goal will contribute to the stakeholder drivers.

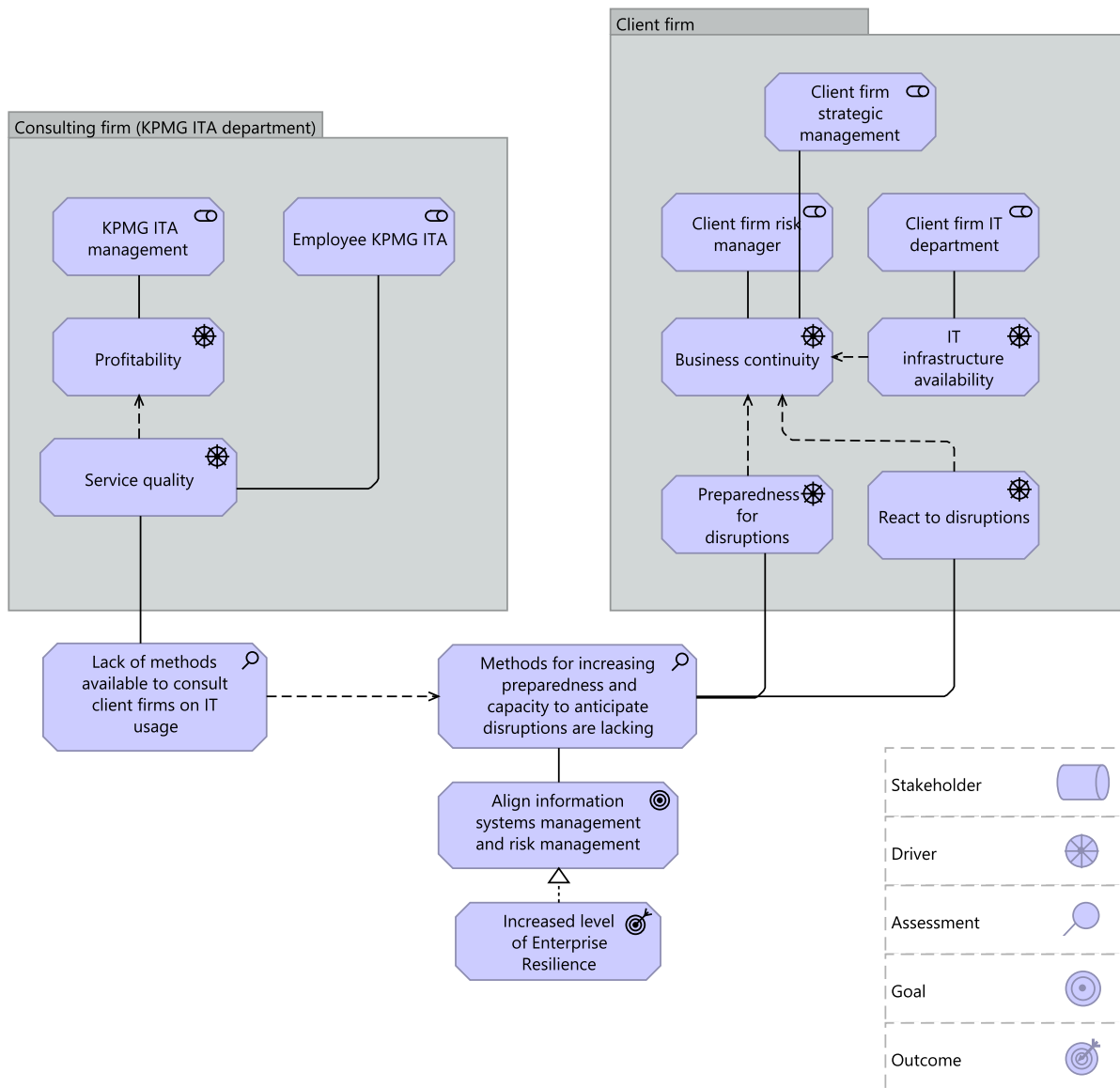


Figure 1: Stakeholders, drivers, and goals for increasing Enterprise Resilience

The main goal is represented at the bottom of Figure 1. In ArchiMate, a goal element represents a desired end state for an organization and its stakeholders. The goal of the involved stakeholders is to **align Information Systems Management and Risk Management with the outcome of improved ER of a client firm**. This goal is linked to what drives the stakeholders. Inherently, the driver of the KPMG IT assurance department management is profitability. This can be increased partly by improving the service quality of their department,



one way to do this is by obtaining additional resources that can assist their employees. A way of increasing service quality to clients is by offering them resources that assist them in IT usage with a reduced level of risk.

The stakeholders that are part of the client firm are driven by ensuring **business continuity**, which can be achieved by investing in a high level of **preparedness** for disruptions and being able to **react** to disruptions (Sanchis et al., 2020). Based on this, an assessment can be made of how all stakeholder drivers can be addressed, which leads to the goal of this research. This results in the assessment that currently **no practical resource is available** for the associated stakeholders that they can apply to achieve increased ER. Therefore, the goal that follows from the stakeholders' motivations is to align Information Systems Management and Risk Management to achieve improved ER at the client firm. Figure 1 shows an increased level of ER as the outcome of aligning Information Systems Management and Risk Management, however, this is the desired outcome and has yet to be validated as a result of this research.

## 1.4 Research questions

The main objective of this thesis is to propose a method to be used by businesses, that aligns aspects from the fields of Risk Management and Information Systems Management to achieve increased ER. Each field alone does not have enough influence on the organization, to significantly lift the level of an enterprise-wide capacity like ER (International Organization for Standardization, 2017). This assessment leads to the main research question that is answered in this thesis. The formulation of the research question is based on the Design Science Methodology by Wieringa (2014), which is discussed in more depth in section 2.1. The research question is formulated as follows:

RQ1: “How to design an **alignment method** between **Information Systems Management** and **Risk Management** to achieve increased **Enterprise Resilience**, that is **practically usable** and **scaled to the risk environment** of an enterprise?”

The main research question (RQ1) gives structure to the goal of this research. It leads to several sub-questions that all contribute to finding an answer to the main research question and will thus serve as guidelines for answering RQ1. Questions RQ1.1-RQ1.5 are concerned with gathering knowledge on the relevant topics and further investigation to get an advanced understanding of the problem context. All questions can be divided into three phases which are problem investigation (RQ1.1-RQ1.5), treatment design (RQ1.6-RQ1.8), and treatment validation (RQ1.9).

---

RQ1.1: “What is **Information Systems Management** and how does it relate to Enterprise Resilience?”

Defining the concept of Information Systems Management based on the latest available literature serves as the foundation for performing research on the concept. A clear definition must be formed that is followed throughout this research. Furthermore, the relationship between Information Systems Management and ER that is described in the literature is examined to serve as a starting point for alignment.

RQ1.2: “What is **Risk Management** and how does it relate to Enterprise Resilience?”

Answering RQ1.2 serves a similar purpose as RQ1.1. A clear definition of Risk Management is necessary to build a novel method around it. Also, the relationship between Risk Management and ER must be examined in the literature to serve as a foundation for designing the alignment method.

---

RQ1.3: “What **treatments are currently available** for achieving increased Enterprise Resilience using Information Systems Management or Risk Management?”

As is discussed in section 3.1, no exact treatments are available that fulfil the requirements of answering RQ1. Therefore, this research attempts to fill a gap in the literature. However, to align the concepts of Information Systems Management and Risk Management, aspects from both must be taken from existing treatments that individually are effective at achieving increased ER, to ensure the alignment method itself is based on effective available treatments. Exploring available treatment is also a step in the *treatment design* stage from the design cycle by Wieringa (2014), which is the chosen methodology in regard to this research. The methodology is discussed further in section 2.1.

---

RQ1.4: “What **enterprise qualities** lead to improved Enterprise Resilience?”

By exploring the enterprise qualities that lead to ER, a better understanding of can be achieved on why certain treatments are effective. This allows us to motivate why any available treatments discovered through RQ1.3 are effective. As well as any other new treatments that are designed during this research.

---

RQ1.5: “What **stakeholders** are involved with Information Systems Management and Risk Management at the **level appropriate for improving Enterprise Resilience**, and is this the strategic, tactical, or operational level?”

While designing a method to assist companies in achieving increased ER, the stakeholders that are applying the method, or are impacted by it, must be identified. During the identification of stakeholders that are concerned with Information Systems Management and Risk Management, the business level at which they affect ER must be uncovered. At this level, the method must be implemented.

Questions RQ1.6-RQ1.8 are part of the next phase of the research, they are focused on the design of the method which includes defining the requirements for it and the execution of the design phase.

---

RQ1.6: “What are the **functional requirements** for an alignment method between Information Systems Management and Risk Management aimed at achieving increased Enterprise Resilience?”

A system has two types of requirements. It is crucial to define these requirements ahead of the design phase to describe what the system must be. All requirements that are set must contribute to some goal of one of the relevant stakeholder, otherwise, the functionality the requirements describes is useless. A functional requirement defines how the system must work, it describes what its functions and features are. Functional and non-functional requirements are elaborated on in section 4.1.

---

RQ1.7: “What are the **non-functional requirements** for an alignment method between Information Systems Management and Risk Management aimed at achieving increased Enterprise Resilience?”

Non-functional requirements define what the system must be, it describes the general properties of a system. These are the quality constraints that the system must comply with. Determining whether a system has met a non-functional requirement is not as straightforward as a functional requirement. Therefore, indicators for each non-functional requirement must be specified to validate whether the system has met the requirement.

---

RQ1.8: “How can an alignment method be **designed** between Information Systems Management and Risk Management to achieve increased Enterprise Resilience?”

The design execution of the alignment method represents the primary objective of this research as it culminates in the creation of the artefact. However, it is important to note that this execution phase constitutes only a single component of the broader Design Science Methodology (Wieringa, 2014) that is employed in this study. Drawing from the requirements and existing knowledge derived from the literature and available treatments, a design process must be undertaken. Given the iterative nature of the Design Science Methodology, the design of the method will unfold across multiple iterations.

---

RQ1.9: “How **effective** is the developed alignment method in practice?”

The last phase consists of only sub-question RQ1.9 which is concerned with the validation of the design.

To iteratively design the method, each version must be validated so it can be overhauled in the next iteration. RQ1.9 is concerned with the validation of the different iterations of the design and eventually validating the final iteration that follows from this research. Validation is also a crucial phase of the Design Science Methodology (Wieringa, 2014).

---

## 1.5 Thesis structure

Firstly, the research design is introduced, which describes the main methodology that is applied to the design of the method. This methodology is the Design Science Methodology by Wieringa (2014) which is based on an engineering cycle consisting of four phases: problem investigation, treatment design, treatment validation, and treatment implementation. The first three phases are executed and reported on in this thesis, the treatment implementation is outside of the scope. The engineering cycle offers an iterative design method, meaning the different phases are to be revisited to continuously improve the method.

Furthermore, the research design expounds upon the research methodologies employed for data collection. A systematic literature review is conducted to acquire data from existing scholarly works. Additionally, semi-structured interviews are conducted to gather insights from expert practitioners in the relevant field. Finally, case studies are conducted, aiming to apply the method to a real-world scenario to simulate its implementation.

After introducing the research design, background knowledge is reported on following the systematic literature review, and the latest reports on existing relationships connected to the research topic are examined to get an understanding of the current state-of-the-art to build upon.

Subsequently, the requirement analysis is presented, encompassing the complete set of requirements that the final version of the method must adhere to. Moreover, methodological considerations relevant to the initial iteration of the method are explicated.

Building upon this foundation, the comprehensive development process regarding the method is delineated. This entails multiple iterations of design and subsequent validation. The validation mechanism employed involves conducting several rounds of interviews with expert practitioners. The insights garnered from these interviews inform the refinement of the method, leading to the culmination of the 'ER enhancement method' in its entirety.

Subsequent to the method's comprehensive development, the credibility of the developed method is established during the final validation phase. Two instruments are employed for this purpose. Firstly, an assessment is conducted to evaluate the adherence of the method to the pre-specified requirements. Secondly, the method is subjected to testing in a simulated setting through the use of case studies. These activities collectively serve to affirm the robustness and effectiveness of the developed method.

After the final method is presented, a discussion on the entire research endeavour is provided, followed by the conclusion.

---

## 2 Research design

---

This thesis attempts to design an information systems artefact. A suitable methodology must be selected for this purpose, the Design Science Methodology by Wieringa (2014) offers such a methodology that describes how to solve design problems iteratively and how to answer knowledge questions. The Design Science Methodology covers all phases of a design process, during this process other methodologies are applied at different phases. To gather knowledge on the topics and lay the foundation for this research, a systematic literature review was performed according to the methodology formulated by Kitchenham and Charters (2007). Additionally, semi-structured interviews are conducted, also case studies are performed for the purpose of validation.

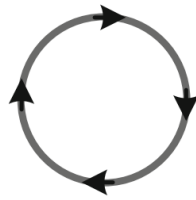
### 2.1 Design science methodology

Design science is the design and investigation of artefacts in context. Wieringa (2014) defined a methodology known as the Design Science methodology that guides researchers in design science. Artefacts are what is designed to interact with a problem context in order to improve something in that context. The investigation into the artefact is done by answering knowledge questions, which are questions about the world as it is. The design of the artefact is done by means of solving a design problem. Design problems assume context and stakeholder goals and aim at designing an artefact such that the interaction between the artefact and the context helps stakeholders achieve their goals. The design problem for this research is described in section 2.1.1.

To solve such a design problem an iterative process known as the engineering cycle is used. The engineering cycle is a rational problem-solving process consisting of the following phases:

- Problem investigation: Explore what phenomena must be improved and why;
- Treatment design: Design an artefact that could treat the problem;
- Treatment validation: Verify whether the design treats the problem;
- Treatment implementation: Treat the problem with the designed artefact;
- Implementation evaluation: Evaluate the success of the treatment, this may be the start of a new iteration through the engineering cycle and is a re-evaluation of the problem investigation phase.

The engineering cycle is visualized in Figure 2, it shows how the process is iterative and may reinitiate after the treatment implementation phase. However, treatment implementation involves deploying the artefact in the real world. This is outside the scope of this research, therefore, a reduced version of the engineering cycle is applied. This means if it is concluded during treatment validation another iteration is required, the treatment implementation is skipped and the process moves on to the implementation evaluation/problem investigation once more. Section 2.1.2 describes in detail how the phases of the cycle are executed by defining the design plan conforming to the adapted engineering cycle.

**Treatment implementation****Implementation evaluation /  
Problem investigation**

- Stakeholders? Goals?
- Conceptual problem framework?
- Phenomena? Causes, mechanisms, reasons?
- Effects? Contribution to Goals?

**Treatment validation**

- Artifact X Context produces Effects?
- Trade-offs for different artifacts?
- Sensitivity for different contexts?
- Effects satisfy Requirements?

**Treatment design**

- Specify requirements!
- Requirements contribute to Goals?
- Available treatments?
- Design new ones!

*Figure 2: Engineering cycle (Wieringa, 2014)*

The cycle starts with problem investigation. During this phase, preparation is done for the design of a treatment by learning more about the problem to be treated. It is about understanding the environment in which the problem must be solved. It consists of detecting the relevant stakeholders by discovering what they want to accomplish. The goals of all stakeholders should lead to assessments of what can be improved. Based on this assessment and the related phenomena and effects, a thorough understanding of the problem can be achieved. This provides an excellent foundation for trying to find a solution to the problem during the treatment design phase.

The goal of this research is to treat a real-life problem. Therefore, Wieringa (2014) uses the term ‘treatment design’ for the conceptualization of a solution, since it suggests an artefact interacting with a problem context to treat a problem. The treatment design phase starts with defining the requirements that the resulting artefact should adhere to. These requirements should contribute to the goal of the relevant stakeholders, otherwise, they are redundant. Following the specification of the requirements, a design must be made that treats the problem according to these requirements. A new treatment can be designed based on available treatments from the literature or practice that touch upon similar problems. When an artefact has been designed, it must be validated during the treatment validation phase.

Treatment validation involves examining the effectiveness of the artefact by justifying that it would contribute to stakeholder goals if implemented. As well as exploring whether the effects of the artefact satisfy the requirements that were set. The alternative usage of the engineering cycle that is used in this research skips the treatment implementation phase and is referred to as the design cycle. So, if signals appear during the treatment validation that improvement is possible, the process returns to the implementation evaluation/problem investigation phase. This means the problem is re-examined to detect possible flaws, which is then followed by another round of design and validation. This process can be iteratively restarted as many times as needed or as many times as resources allow.

### 2.1.1 Design problem

Wieringa (2014) defines a design problem as a problem to (re)design an artefact so that it better contributes to the achievement of some goal. In the Design Science Methodology, the design problem acts as the central problem that has to be treated. Design problems assume a context and stakeholder goals and call for an artefact such that the interactions of an artefact

with the problem context help the relevant stakeholders to achieve their goals. The problem context describes what the artefact interacts with and what needs to be improved. The design science methodology provides a template for defining the design problem:

Improve **<a problem context>**...  
 ...by **<(re)designing an artefact>**...  
 ...that satisfies **<some requirements>**...  
 ...in order to **<help stakeholders achieve some goals>**.

This section describes the design problem that was formulated, which acts as the main objective to achieve for this research. The design problem was rewritten as a research question and was described in section 1.2 as RQ1.

Improve **the level of Enterprise Resilience**...  
 ...by **designing an alignment method between Information Systems Management and Risk Management**...  
 ...that **is practically usable and scaled to the risk environment of an enterprise**...  
 ...in order to **provide firms with a tool to make increasing Enterprise Resilience more attainable and make consultation easier for consulting firms, such that they can be more competitive**.

The problem context is the level of ER. Since the goal is to improve the level of ER of the firm that utilizes the method. We want to improve this problem context by (re)designing an artefact, which is an alignment method between Information Systems Management and Risk Management.

The artefact has to conform to some requirements to ensure that the artefact serves a useful purpose. A complete list of exact requirements is specified in section 4.1. The design problem only specifies the global requirements that define the general behaviour of the artefact. For the design of the artefact during this research, the method must be applicable in practice. During the SLR (chapter 3), a lack of practically applicable methods for achieving ER was observed. Therefore, a global requirement for the design of the artefact in this research is to ensure that it can be applied by firms in practice. This is opposite from most other work on the subject which is often more conceptual and does not provide practical instructions for firms (Pettit, Fiksel, & Croxton, 2010; Sanchis et al., 2020; Woods & Wreathall, 2003). Furthermore, the artefact must apply to firms that operate in different risk environments. Risk environments can differ based on the size of a firm, the sector they operate in, the size of its supply chain, or even the complexity of its IT estate. The goal of this research is to design a method that does not focus on any of these aspects specifically but instead operationalizes suitable aspects from Information Systems Management and Risk Management in a way that the strategic direction of a firm will include resilience building at its core.

Designing this artefact should contribute to the goals of stakeholders. The key stakeholder is the firm, thus the method aims at providing a tool to this firm that allows them to increase their

level of ER. Besides this, the goal of the consulting firm (KPMG) is to make consulting easier, so they can be more competitive.

## 2.1.2 Design plan

The design of the artefact is structured according to the design cycle. The design plan, along with the methodologies that are used in each of the phases are visualized in Figure 3. The phases of the design cycle are followed in sequences but iteratively continue after the treatment validation if another cycle is necessary.

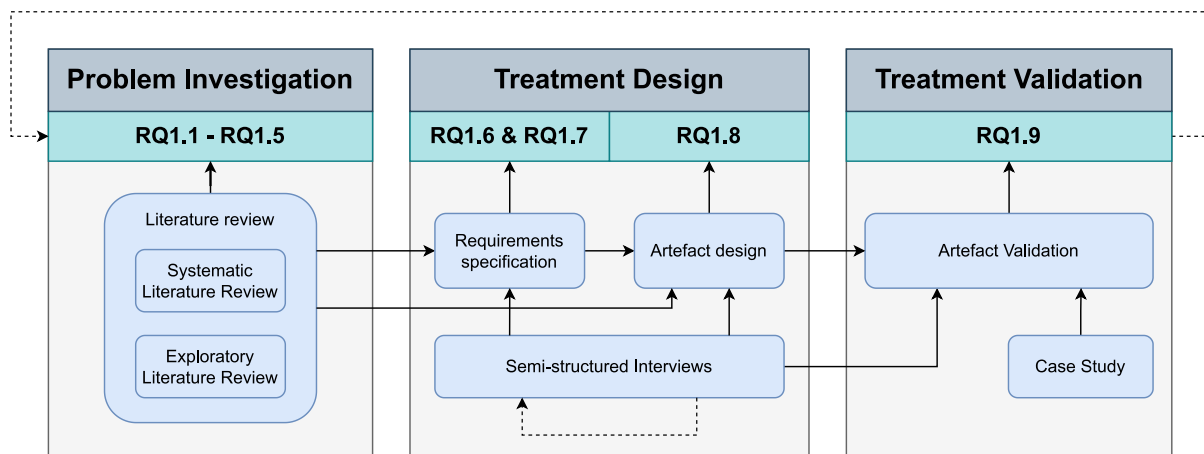


Figure 3: Research process mapped on the design cycle by Wieringa (2014)

The first phase is the problem investigation phase, which covers RQ1.1 to RQ1.5:

RQ1.1: “What is **Information Systems Management** and how does it relate to Enterprise Resilience?”

RQ1.2: “What is **Risk Management** and how does it relate to Enterprise Resilience?”

RQ1.3: “What **treatments are currently available** for achieving increased Enterprise Resilience using Information Systems Management or Risk Management?”

RQ1.4: “What **enterprise qualities** lead to improved Enterprise Resilience?”

RQ1.5: “What **stakeholders** are involved with Information Systems Management and Risk Management at the **level appropriate for improving Enterprise Resilience**, and is this the strategic, tactical, or operational level?”

These questions cover the understanding of the problem. According to the Design Science Methodology by Wieringa (2014), these questions are considered *knowledge questions*. Knowledge questions do not ask for a change in the world but ask for knowledge about the world as is. Therefore, these questions are answered using a literature review, since this involves gathering existing knowledge about the world as is. The exact methodology for the literature review is outlined in section 2.2.1.



This is followed by the treatment design phase, which involves the design activities and is covered by answering RQ1.6, RQ1.7, and RQ1.8:

---

RQ1.6: “What are the **functional requirements** for an alignment method between Information Systems Management and Risk Management aimed at achieving increased Enterprise Resilience?”

RQ1.7: “What are the **non-functional requirements** for an alignment method between Information Systems Management and Risk Management aimed at achieving increased Enterprise Resilience?”

RQ1.8: “How can an alignment method be **designed** between Information Systems Management and Risk Management to achieve increased Enterprise Resilience?”

---

Firstly, the requirements must be defined. Requirements follow from the desires of stakeholders, so requirements are partly specified using the findings from RQ1.1-RQ1.5. Especially the answer to RQ1.5 on stakeholders is relevant for specifying requirements. Additionally, requirements can be specified as a result of interviews with experts. This allows the opinions of stakeholders to be heard and reflected in the requirements. The interviews are semi-structured, this methodology is described in more detail in section 2.2.2. Consequently, the requirements lead to the constraints and the goals that the design of the artefact must adhere to.

The initial design of the artefact is based on available treatments in literature and practice. Aspects from different treatments are combined to form an initial artefact that can be improved iteratively following the design cycle. The insights needed to improve the artefact are gathered from the semi-structured interviews with experts.

Next, the design must be validated during the treatment validation phase, which is covered by RQ1.9:

---

RQ1.9: “How **effective** is the developed alignment method in practice?”

---

The artefact is validated partly through expert opinion in semi-structured interviews. Also, case studies are performed aiming at validating the artefact using a real case to approach practical validation. The combination of the results from these activities determines whether another round of the design cycle must be started to achieve the optimal result. However, there are constraints like time and resources that may limit the number of cycles.

### 2.1.3 Design cycles

Throughout this research endeavour, the design cycle depicted in Figure 2 is iterated through multiple times. Table 1 outlines the activities performed during each cycle, encompassing problem investigation, treatment design, and treatment validation. Notably, the scope of this research excludes treatment implementation.

Cycle 1 encompasses the initial design phase, which is formulated based on insights derived from relevant literature and available treatments pertaining to the research problem. This design is subsequently validated through interviews conducted with domain experts, aiming to acquire fresh perspectives and feedback regarding the initial method.

Cycle 2 entails revisiting the initial problem and redesigning the method in light of the insights gained from the validation process of the previous cycle. The improved method is then subjected to validation via further expert interviews.

Cycle 3 follows a similar design phase, where the method is further refined based on the outcomes of previous validation activities. To achieve validation in this cycle, a comprehensive case study is performed, aiming to closely approximate real-world testing of the method's effectiveness.

During the treatment validation phase within each cycle, thorough checks are conducted to ensure that the method adheres to the specified requirements.

*Table 1: Design cycle activities*

<b>Cycle</b>	<b>Problem investigation</b>	<b>Treatment design</b>	<b>Treatment validation</b>
1	Stakeholder analysis & Literature review	Design initial artefact using literature and available treatments	1 <sup>st</sup> round of interviews with experts & Requirement satisfaction
2	Re-evaluate stakeholder drivers and goals	Redesign based on cycle 1 validation	2 <sup>nd</sup> round of interviews with experts & Requirement satisfaction
3	Re-evaluate stakeholder drivers and goals	Redesign based on cycle 2 validation	Case study & Requirement satisfaction

## 2.2 Research methodologies

The following section specifies the methodologies that were used for executing this research. To examine existing literature the Systematic Literature Review by Kitchenham and Charters (2007) is used. Furthermore, expert opinions were collected through interviews, specifically semi-structured interviews. And a case study was performed to observe how effective the method would be when applied to a real case.

### 2.2.1 Systematic literature review

Existing knowledge that contributes to answering the research questions must be gathered through a literature review of academic works. This requires a methodology that ensures data is gathered in an unbiased manner, which leads to a result that is a true reflection of the latest findings on a certain topic. The Systematic Literature Review methodology by Kitchenham and Charters (2007) aims at accomplishing this. Their goal was to design a systematic review for performing rigorous reviews of current empirical evidence to the software engineering community. It is primarily aimed at research in the field of software engineering. The topics discussed in this research go beyond solely software engineering but aspects of it are included. For that reason, in combination with the rigorous and unbiased nature of the method, the

Systematic Literature Review is a suitable methodology. A more in-depth explanation of how the method works can be found in section 3.1.

## 2.2.2 Interview

When the main objective of the researcher is to better understand the participant's unique perspective on a phenomenon, semi-structured interviews are generally the preferred data collection method (Adeoye-Olatunde & Olenik, 2021). A semi-structured interview is a qualitative research method that is based on a set of pre-determined open questions, but the researcher allows the interviewees to further explore topics of their choosing, intending to engage in a more loose and flexible conversation. The goal of the interviews in the context of this research is to gather knowledge on a phenomenon which is not yet fully mature, this being ER as described in section 3.2.1. Semi-structured interviews permit the interviewees to be focused on a certain topic, while still allowing the researcher to explore new aspects that the interviewee can introduce during the conversation. It should allow the researcher to get deeper insights into the perspective of the interviewee by allowing interviewees to provide new knowledge not in the pre-determined set of questions.

Adeoye-Olatunde and Olenik (2021) specify a methodological approach to semi-structured interviews. They describe seven steps to conducting, analysing, and reporting semi-structured interview data which are shown in Table 2, along with the sub-topics that should be addressed. The methodology was originally written for pharmacy services research, however, it is stated by the authors that it can be applied to various types of research.

*Table 2: Seven steps to conducting, analysing, and reporting semi-structured interview data (Adeoye-Olatunde & Olenik, 2021)*

<b>Steps</b>	<b>Sub-topics</b>
1	Assess the appropriateness of the semi-structured interview
2	2a. Sampling approaches 2b. Recruitment
3	3a. Developing the semi-structured interview guide 3b. Collecting participant demographic information
4	4a. Preparation and training 4b. Interview modality and recording considerations 4c. Transcription and checking 4d. Securely storing and transmitting data
5	5a. Coding and theme identification 5b. Establishing rigour
6	Drawing conclusions
7	7a. Reporting guidelines 7b. Data display

Step 2 is concerned with sampling and participant recruitment. Non-probability sampling was used for the selection of participants, more specifically purposive sampling. This is an approach

for purposive selecting of participants based on meeting certain criteria of interests, the profiles that describe the desired candidates for interviews are shown in Appendix A.

The set of questions that were defined for the interviews can be found in Appendix B which is a part of step 3. It also specifies which demographic information is collected. The following information was requested to create a profile for each participant while ensuring their anonymity: their job title, years of experience, the sector their company operates in, and the number of employees at their company.

Step 4 is partly concerned with recording and data storing considerations. The interviews were conducted in the form of video calls using Microsoft Teams. Only the audio of each interview was recorded. The recordings were purely stored locally and were erased after they were processed.

During steps 5, 6, and 7 the audio recordings of the interviews are transcribed and coded to identify similarities and differences in the interview data. Finally, a conclusion is drawn from the data and presented and reported.

### 2.2.3 Case study

In consideration of the thesis's scope, it is important to note that the treatment implementation phase of the design cycle, as outlined by Wieringa (2014), will not be encompassed. Nevertheless, the most effective means of validating the research findings is through real-world implementation, allowing for insights to be gathered from users who would be actively applying the method. To simulate this implementation, qualitative case studies are conducted to evaluate the artefact within its specific problem context. Baxter and Jack (2008) assert that a qualitative case study is well-suited for facilitating the exploration of a phenomenon within its context.

According to Baxter and Jack (2008), the initial step in conducting a qualitative case study involves determining the case or unit of analysis. It is imperative to ascertain the specific aspects that the researcher intends to analyse, which, in the context of this research, pertains to the impact of the method on the level of ER before, during, and after a significant disruption. Subsequently, the case must be bounded by establishing limitations to ensure it remains focused and does not become too broad. These boundaries can be set in terms of time, location, or included activities. By appropriately defining these boundaries, the case study maintains a reasonable scope.

Determining the type of case study is also crucial. An explanatory case study is well-suited for this research, as it enables the exploration of presumed causal links within complex real-life interventions that cannot be adequately addressed through surveys or interviews alone. Additionally, a multiple case study design can be adopted to examine more than one case, facilitating a deeper understanding of the methodology's effectiveness in different contexts.

## 2.3 Summary

This chapter of the thesis focuses on describing the research design, which involves describing the primary design methodology, as well as describing the methodologies used for data collection. The Design Science Methodology by Wieringa (2014) is chosen as the methodology for solving design problems iteratively and answering knowledge questions. This methodology covers all phases of the design process, with other methodologies applied at different stages.

To establish a foundation for the research, a systematic literature review is conducted following the methodology formulated by Kitchenham and Charters (2007).

The Design Science Methodology, as defined by Wieringa (2014), involves designing and investigating artefacts in a specific context to improve the existing situation. The investigation of the artefact is carried out by answering knowledge questions, while the design process aims to solve a design problem within the given context.

The design cycle is used as an iterative process to solve design problems, consisting of problem investigation, treatment design, treatment validation, and treatment implementation. However, the treatment implementation phase is outside the scope of this research, so a reduced version of the design cycle is applied. If it is determined during treatment validation that further iterations are required, the process returns to the implementation evaluation/problem investigation phase.

The chapter then details the design problem formulated for the research, which aims to improve the level of ER by designing an alignment method between Information Systems Management and Risk Management. The design plan is structured according to the design cycle, with different research questions guiding each phase of the process.

The methodologies employed in this research include a systematic literature review following the methodology by Kitchenham and Charters (2007), semi-structured interviews to gather expert opinions, and a case study to validate the effectiveness of the designed method.

---

## 3 Literature review

---

With the overarching goal of aligning Information Systems Management and Risk Management to achieve resilience, this chapter provides a comprehensive review of the available literature on the aforementioned topics. The topics of Enterprise Resilience, Information Systems Management, and Risk Management are analysed separately. Followed by an examination of the relationships between Information Systems Management and Enterprise Resilience, as well as Risk Management and Enterprise Resilience. A systematic literature review is performed on these relationships to obtain an unbiased and thorough result. Aiming at finding an overlap between Information Systems Management and Risk Management and their relationship to Enterprise Resilience, the findings are used as the foundation for the design of an alignment method.

### 3.1 SLR Methodology

To perform a robust literature review, a methodology must be selected and followed to ensure that the result is representative of the source literature. One such methodology is presented by Kitchenham and Charters (2007), who provide guidelines for performing systematic literature reviews in software engineering. A systematic literature review (SLR) is a method used to identify, evaluate, and interpret all relevant research on a research question, topic area, or phenomenon of interest. What makes an SLR rigorous is the focus on thoroughness and fairness, to provide an unbiased result. This can be achieved by defining a search strategy beforehand, to only select literature that is the result of an unbiased search query. Instead of hand-picking the literature, which can lead researchers to select literature that might support their preferred hypothesis, which results in a biased review.

The method provided by Kitchenham and Charters (2007) consists of three phases, each containing several stages. The three main phases are:

- Planning the review
- Conducting the review
- Reporting the review

All activities performed during each phase are described below.

#### 3.1.1 Planning the review

After the need for a review was confirmed by trying to identify any previous research into the topic, the first step was to define the research questions that are answered using the SLR. While examining whether any previous literature reviews were performed on aligning Information Systems Management and Risk Management to achieve ER, it was found none had been done. Therefore, the goal of the literature review is instead split up into two research questions. Gathering answers to these questions forms the basis for alignment, the questions are:

**RQ1.1:**What is Information Systems Management and how does it relate to Enterprise Resilience?

**RQ1.2:**What is Risk Management and how does it relate to Enterprise Resilience?

To ensure the accuracy and unbiasedness of the review, part of the planning is to develop a research protocol. A research protocol specifies the exact steps that are to be taken, this includes the selection of literature databases, defining the search queries, defining study inclusion- and exclusion criteria, and defining the study quality assessment procedure. These activities are carried out in the next phase, conducting the review. During the review, the research protocol was followed and thus the details of each activity are presented in the next section alongside the results of the activity.

## 3.1.2 Conducting the review

### 3.1.2.1 Literature database selection

To obtain relevant academic publications, reputable online scientific databases were selected as sources for the literature. They were selected based on the research fields that are covered, the total coverage of items, and their reputation. The utilized databases can be seen in Table 3.

*Table 3: Scientific databases*

Database	URL	Discipline
IEEE Xplore	<a href="https://ieeexplore.ieee.org/">https://ieeexplore.ieee.org/</a>	Engineering & Computer Science
Science Direct	<a href="https://www.sciencedirect.com/">https://www.sciencedirect.com/</a>	Multidisciplinary
Scopus	<a href="https://www.scopus.com/">https://www.scopus.com/</a>	Multidisciplinary
Google Scholar	<a href="https://scholar.google.com/">https://scholar.google.com/</a>	Multidisciplinary

### 3.1.2.2 Search query formulation

To answer the formulated research question, search queries had to be formulated. Each database has its specific syntax, which means slightly different queries are specifically required for each database. To answer RQ1.1 the two main components are used as keywords:

- 'Information systems management'
- 'Enterprise resilience'

Similarly, answering RQ1.2 requires the use of the two keywords:

- 'Risk management'
- 'Enterprise resilience'

To cover each keyword entirely, the search queries were expanded by including synonyms and utilizing the wildcard functionality on each database. For example, synonyms used for 'information systems management' were: 'information system', 'Information technology', and 'information communication technology'. Moreover, wildcards can be used to allow search results to be selected that can be spelt or formulated slightly differently. For example, 'information system\*' was used to include results that contained a variation of the term, like 'systems'.

The two search queries that were formulated are presented below. All databases have implemented syntaxes of their own, which all vary slightly from each other. The most basic



search queries for the research questions are presented below, for each database, a similar search query was used depending on the syntax.

**RQ1.1:** (“*Information system\**” OR “*Information technolog\**” OR “*Information communication technolog\**”) AND “*Enterprise resilience*”

**RQ1.2:** “*Risk management*” AND “*Enterprise resilience*”

Each query results in a set of articles that is examined further.

### 3.1.2.3 Selection criteria

Ahead of the search process, selection criteria were defined to reduce the likelihood of bias in the selection of articles. Both inclusion- and exclusion criteria were defined to filter out any articles that do not meet any standards necessary to be included in the review. These criteria are included in Table 4. Thus, articles that comply with the inclusion criteria are integrated into the review, if they are not excluded by any of the exclusion criteria.

Firstly, the articles need to cover the topics defined in the research questions. Thus, for search query 1, the article must cover Information Systems Management and its relation to Enterprise Resilience. Similarly, articles resulting from search query 2 need to cover Risk Management and its relation to Enterprise Resilience. Articles must also be published in conference proceedings or a scientific journal.

The exclusion criteria are used to filter out any articles that comply with the inclusion criteria but do not meet the standard necessary for ensuring an SLR of quality. So, the publishing date is considered. The fields of ‘Information Systems Management’ and ‘Risk Management’ are very mature, while research on Enterprise Resilience does not date this far back. For this reason, articles cannot be older than 15 years. This cut-off point was determined by considering the number of papers published on the topics over the years.

*Table 4: Selection criteria*

Inclusion criteria	Exclusion criteria
For search query 1: Covers the topic ‘Information Systems Management’ and its relation to ‘Enterprise Resilience’	Paper is not written in English
For search query 2: Covers the topic ‘Risk Management’ and its relation to ‘Enterprise Resilience’	Paper is older than 15 years
Published in a reputable journal or conference	Paper is a duplicate on the same research, only the most complete and recent paper is considered
Paper is peer-reviewed	
Paper reports on full research, no extended abstract allowed	

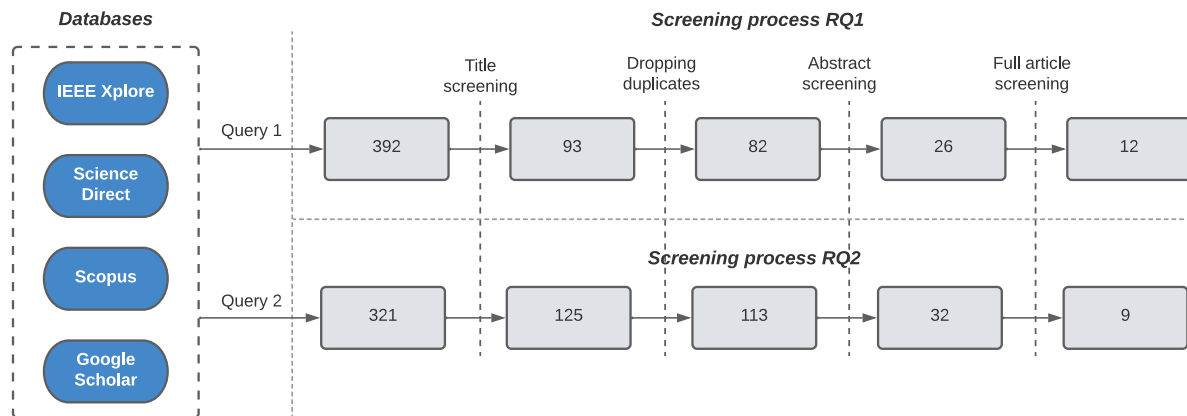
### 3.1.2.4 Article selection

The previous chapters have defined the review protocol that serves as the basis for the SLR. Starting with the definition of the research questions, followed by the selection of the scientific databases to be used, then the search queries were defined, and eventually the selection



criteria as well. Next, to collect the resulting articles from the different databases, the search results were exported to files compatible with the importation into EndNote. The resulting articles should all have some connections with at least one of the two research questions. However, more careful examination is needed to ensure the articles are suitable.

The search query for RQ1.1 resulted in 392 articles collected from the different databases. Firstly, they underwent a title screening, in which unrelated articles were excluded based on just the title. This resulted in 93 remaining articles. Since different databases can contain the same articles, duplicates were removed which resulted in 82 remaining articles. This was followed by a closer look at the abstracts, which reveal more about the full contents of the article. Screening the abstracts resulted in 26 articles. To ensure the articles are suitable for the review, a final full article screening was performed. Reading the full articles was directly combined with data extraction in case the article was serviceable for the review. Data extraction refers to recording the information from the article that is deemed useful for the review. The final article selection consists of 12 remaining articles. The same method was applied to the resulting articles from the query for RQ1.2. The complete article selection process for RQ1.1 and RQ1.2 is visualized in Figure 4.



**Figure 4: Screening process RQ1.1 & RQ1.2**

Using the collected articles, the following chapters present all relevant collected data on the topics. The goal of these chapters is to answer the research questions and as a result, present an overview of the topics. The final selection of papers for RQ1.1 is presented in Table 5, and the final selection for RQ1.2 is presented in Table 6.

**Table 5: RQ1.1 article selection**

Reference	
1	Ciampi, Marzi, and Rialti (2018), Artificial intelligence, big data, strategic flexibility, agility, and organizational resilience: A conceptual framework based on existing literature
2	Conz and Magnani (2020), A dynamic perspective on the resilience of firms: A systematic literature review and a framework for future research
3	Erol et al. (2010), A framework for investigation into extended Enterprise Resilience
4	Gomes (2015), Resilience and enterprise architecture in SMEs

5	Heeks and Ospina (2019), Conceptualising the link between information systems and resilience: A developing country field study
6	Ignatiadis and Nandhakumar (2007), The impact of enterprise systems on organizational resilience
7	Madani and Parast (2023), An integrated approach to organizational resilience: a quality perspective
8	Mallak and Yildiz (2016), Developing a workplace resilience instrument
9	Schemmer, Heinz, Baier, Vössing, and Kühn (2021), Conceptualizing Digital Resilience for AI-based Information Systems
10	Thiede, Fuerstenau, and Bezerra Barquet (2018), How is process mining technology used by organizations? A systematic literature review of empirical studies
11	Velu, Al Mamun, Kanesan, Hayat, and Gopinathan (2019), Effect of information system artifacts on organizational resilience: A study among Malaysian SMEs
12	D. Wang and Chen (2022), Digital Transformation and Enterprise Resilience: Evidence from China

*Table 6: RQ1.2 article selection*

<b>Reference</b>	
1	Assibi (2022), The Role of Enterprise Risk Management in Business Continuity and Resiliency in the Post-COVID-19 Period
2	Buganová, Mošková, and Šimíčková (2021), Increasing the Resilience of Transport Enterprises through the Implementation of Risk Management and Continuity Management
3	Hudakova and Lahuta (2020), Risk Management as a Tool for Building a Resilient Enterprise
4	Lisdiono, Said, Yusoff, and Hermawan (2022), Risk management practice, alliance management capability, and Enterprise Resilience: Findings from Indonesian state-owned enterprises
5	Oh and Teo (2009), An empirical study of IT-enabled enterprise risk management and organizational resilience
6	Pettit, Fiksel, Polyviou, and Croxton (2014), Embracing Change: From Risk to Resilience
7	Rohmeyer and Zvi (2009), Risk management decision making in ICT for development
8	Skulimowski and Łydek (2022), Applications of AI Alignment and Anticipatory Networks to Designing Industrial Risk Management Decision Support Systems
9	Teoh and Zadeh (2013), Strategic resilience management model: Complex enterprise systems upgrade implementation

## 3.2 Definitions

Before answers to the research questions can be given, clear definitions of the primary areas of interest must be present. In this chapter, definitions, and descriptions from the literature for ER, Information Systems Management, and Risk Management are given. For each topic, a concluding definition is presented that is utilized in the remainder of this research. Sources that were used to define the topics were not subject to the SLR, so other external sources were

utilized. The reason for this is that papers resulting from the SLR are focused on the relations between IS Management, Risk Management, and ER. This excludes a large number of papers solely focused on ER which are likely to contain the state of the art. To include them, an exploratory search for papers was executed alongside the SLR for the definitions in this chapter. Papers resulting from the exploratory search were selected based on the number of citations, their recency, and relevancy.

### 3.2.1 Enterprise Resilience

Enterprise Resilience has been studied at different levels, the company as a whole has been considered as the subject, but it also has been studied at the individual level, where the individuals working in an enterprise are the subject. Furthermore, the term also has been applied at the supply chain level (Bak, Shaw, Colicchia, & Kumar, 2023). It is suggested by Madani and Parast (2023) that an enterprise often exists in a supply chain, which means the firm receives inputs from suppliers and delivers outputs to customers. Therefore, they conclude resilience studies at the supply chain level and the company level are applicable to each other, although not equal.

Many definitions of ER have been proposed, but so far, no definition is accepted by all. One definition that considers ER at the company level comes from Sanchis et al. (2020), who define it as the capacity to *anticipate* and be prepared to face disruptive events and, if unavoidable occurrences take place, it also includes the capacity to *recover* as quickly and efficiently as possible. The mentioning of unavoidable occurrences is critical to the definition, ER revolves around occurrences that could negatively impact the enterprise. The definition by Sanchis et al. (2020) mentions both preparedness and recoverability from such negative occurrences as capacities that one should have to obtain ER. This suggests that both *proactive* as well as *reactive* actions are necessary to develop ER. This statement is further strengthened by definitions formulated by Sin and Ng (2013), who describe the evolution of the topic of ER. Initially, ER was defined as organizational tenacity in maintaining positive adjustment under challenging conditions, which suggests that ER is purely reactive. However, they describe how later studies extended the concept to include business continuity, which refers to an enterprise's level of readiness to maintain critical functions. This implies the addition of proactive capabilities. Other studies that mention the separation between proactive and reactive capacity include Madni and Jackson (2009) and Winston (2014). Also, Conz and Magnani (2020) mention ER is an attribute the firm possesses along a continuum: before, during, and after an event.

A study by D. Wang and Chen (2022) divides the topic of ER into two different aspects: (1) the ability to respond to emergencies; and (2) the ability of sustainable development, which is, the ability of that enterprise to continuously adapt, learn, and innovate to achieve a spiral upward. This is another aspect mentioned often in relation to ER; the ability to not only survive adversity but to learn from it – moving beyond the previous states and *emerging strengthened* from experience. Hepfer and Lawrence (2022) describe this aspect as '*bouncing back and bouncing forward*'. However, in their literature review, they found that not all definitions include the concept of bouncing forward, since occasionally only recovering from disruptions is mentioned. Lengnick-Hall, Beck, and Lengnick-Hall (2011) also mention engaging in transformative activities to capitalize on disruptive surprises that threaten organizational survival as a part of ER. Again, the ability to capitalize and thus improve, or 'bounce forward' is mentioned. However, Sanchis et al. (2020) mention that recovering does not necessarily have to lead to an improved situation. In case competitors are also disrupted, which is often the case, it is

necessary to return to a state after recovery at which competitive advantages are maintained, which is not necessarily an improvement of the original situation.

As mentioned before, ER is considered on different levels. Generally, a *company-wide view* is taken that considers different structural levels within a firm, the level of the business processes, the supply chain level, and also the organizational level. Resilience on the organizational level is often defined as *organizational resilience*, which is related to ER. The difference mainly lies, according to most researchers, in the fact that organizational resilience considers mainly management activities. Achieving it involves activities related to human resource management, strategy, leadership, and entrepreneurship (Hepfer & Lawrence, 2022). If ER takes into account the whole enterprise, organizational resilience can be seen as a subset of ER. However, McManus, Seville, Vargo, and Brunsdon (2008) define organizational resilience as a function of an organization's overall situation awareness, management of keystone vulnerabilities, and adaptive capacity in a complex dynamic, and interconnected environment. A similar definition for organizational resilience is given by Hassan, Kushwaha, and Sharma (2022), they say it is the maintenance of positive adjustment under challenging conditions such that the organization emerges from those strengthened and more resourceful. Both definitions do not specifically consider organizational resilience as being purely at the management level. In fact, ER and organizational resilience seem to be considered equal by these authors. However, a careful examination must be made on whether each author refers to organizational resilience on the management- or company-wide level. Moreover, operational resilience constitutes a significant subset of ER. Considering that a substantial portion of disruptions encountered by companies directly impacts their operability, operational resilience is widely regarded as an indispensable component of ER as a comprehensive concept (Allen & Davis, 2010).

It should be noted that companies that want to improve ER have to invest in capabilities. Pettit et al. (2010) mention that investment in these capabilities should be balanced with the level of vulnerabilities faced by the company. This relation is visualized in Figure 5, which shows the concept of *balanced resilience*. Firms should aim to be in the zone of balanced resilience, which means they *avoid eroding their profits* by overinvesting in capabilities, while also limiting their exposure to risks by *matching the investment in capabilities with their level of vulnerability*. The specific capabilities are discussed in the next section.

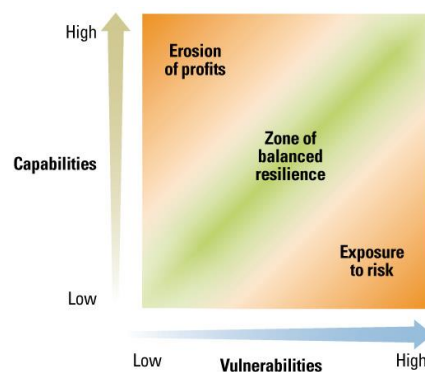


Figure 5: *Balanced resilience* (Pettit et al., 2010)

### 3.2.1.1 Enterprise Resilience qualities

To achieve ER, a company must have certain qualities that contribute towards improving the level of ER. All identified qualities are presented in Table 7. Conz and Magnani (2020) mention

the core qualities of being resilient. They make a distinction between absorptive and adaptive qualities. Absorption of shock occurs as a consequence of a critical event and involves maintaining stability and preserving assets. Adaptation of a shock is when firms recombine extant or novel resources and prompt internal changes. The core absorptive qualities mentioned by Conz and Magnani (2020) are *redundancy*, *robustness*, and *agility*. Ahead of a shock, redundancy is necessary to mitigate the chance of loss of assets, also robustness is needed to resist a shock and to aim at eliminating vulnerabilities in a firm's operating environment. These qualities need to be balanced with each other, as well as with the needed investment to optimize the long-term benefit against an acceptable price (Pal, Torstensson, & Mattila, 2014). If a firm is redundant and robust, it must then be able to actively respond to a shock, which can be achieved by responding with agility. Redundancy and agility are also mentioned as crucial qualities by Erol et al. (2010).

The adaptive qualities mentioned by Conz and Magnani (2020) are *resourcefulness*, *adaptability*, and *flexibility*. Resourcefulness is the quality of a firm to gather different diversified assets and resources. Adaptability is the quality to react dynamically and adapt internal processes to change external conditions (Erol et al., 2010; Sanchis et al., 2020). The effect of these capabilities is strengthened when they can be used flexibly.

Another crucial quality is *situation awareness*, which is the ability to understand and identify changes in the environment of the firm (Erol et al., 2010). Understanding the environment can lead to increased preparedness compared to competitors since a firm that understands its environment can see disruptions coming at an earlier stage (Madani & Parast, 2023; McManus et al., 2008; Teoh & Zadeh, 2013).

The level at which companies manage their strategic partnership portfolio is also relevant to create ER. This is also referred to as *alliance management*. It was found that proactiveness in alliances can lead to ER through increased levels of sustainable innovation and sharing of resources (Lisdiono et al., 2022). This view is shared by Erol et al. (2010) and Madani and Parast (2023), who mention collaboration between allies is an important quality to achieve a higher level of ER.

Table 7: ER qualities

Qualities	Source	Qualitative metrics	Quantitative metrics
Redundancy	(Conz & Magnani, 2020), (Erol et al., 2010), (Heeks & Ospina, 2019), (Madani & Parast, 2023)	Function continuity, resource spareness, functional overlaps and interdependencies, resource substitutability	Safety stock, backup sites, backup IT infrastructure, excess capacity
Robustness	(Conz & Magnani, 2020), (Heeks & Ospina, 2019), (Madani & Parast, 2023)	Shock absorption, multilevel governance	
Agility	(Conz & Magnani, 2020), (Erol et al., 2010), (Madani & Parast, 2023)	Awareness, visibility	Response time

Resourcefulness	(Conz & Magnani, 2020)	Resource diversity	
Adaptive capacity	(Conz & Magnani, 2020), (Erol et al., 2010), (Fiksel, 2016), (McManus et al., 2008), (Sanchis et al., 2020)	Information dissemination, opportunism	Time to equilibrium during instability,
Flexibility	(Conz & Magnani, 2020), (Erol et al., 2010), (Heeks & Ospina, 2019), (Madani & Parast, 2023)	Versatility, responsiveness, decision-making speed	Number of back-up suppliers, contract flexibility, product modularity
Situation awareness	(Erol et al., 2010), (Madani & Parast, 2023), (McManus et al., 2008), (Teoh & Zadeh, 2013)	Stakeholder knowledge	
Alliance management	(Erol et al., 2010), (Lisdiono et al., 2022), (Madani & Parast, 2023)	Level of information sharing, resource reallocation	
Usage of information technologies	(Madani & Parast, 2023), (Sheth & Kusiak, 2022), (D. Wang & Chen, 2022)	Digitalization	
Recovery capacity	(Fiksel, 2016), (Madani & Parast, 2023), (Sanchis et al., 2020)	Maximum tolerable damage	
Vulnerability management	(Fiksel, 2016), (Madani & Parast, 2023), (McManus et al., 2008)		Vulnerability quotient (probability of disruption occurrence, and severity of consequences)
Diversity	(Fiksel, 2016)		Number of qualified sources by component

Proper *usage of information technology and statistical analysis* strengthens business processes, this positively affects predictive, adaptive, and restorative capacities. Which are factors that contribute to increased ER (Madani & Parast, 2023). Especially the application of information technology is crucial because it can improve the level of automation and intelligence, as well as effectively strengthen production efficiency. When a disruption occurs, these advantages enable companies to quickly allocate resources to create opportunities to achieve unconventional growth. Also, information technology allows cross-departmental communication which connects separate business units into a whole. Which results in connection efficiency, bettering the enterprise's emergency response capabilities (Teece, Peteraf, & Leih, 2016).

Another reactive quality is the *recovery capacity*, which is the ability to respond and recover from a disruption which is mentioned as being key for bolstering ER (Madani & Parast, 2023;



Sanchis et al., 2020). Recovery capacity does not always mean returning to the pre-disruption state, the intent during recovery should be to reach a state at which competitive advantages are maintained.

Vulnerabilities are always present in companies, and to *manage vulnerabilities* to the best extent they need to be identified and prioritized (McManus et al., 2008).

*Diversity* in this context refers to having a variety of market suppliers, facilities, and employee capabilities. In case of a disruptive event, having the ability to choose from various resources can decrease the chances of having to halt an operation (Fiksel, 2016).

### 3.2.1.2 Disruptions

The need for ER stems from disruptions that can occur at any moment (Sanchis et al., 2020). It can be defined as a *foreseeable* or *unforeseeable* occurrence, which directly affects the normal operations and stability of a company (Barroso, Machado, & Machado, 2008). Disruptions can have different sources which are often classified as *internal* or *external*. Barroso et al. (2008) classify humans, equipment, energy-related issues, and financial aspects as internal disruptive sources, i.e., aspects originating from the critical infrastructure within an organization. Issues relating to supply, man-made events, government, society, other external stakeholders, and natural events are considered to derive from external disruptive sources (Aldea, Vaicekauskaitė, & Daneva, 2020; Barroso et al., 2008). A disruption can range from a minor incident to a major occurrence that can severely harm a firm.

Disruptions can occur over a few minutes, a few hours, or even a few days. But they generally follow the pattern seen in Figure 6. It shows the impact on the performance of a firm during the three stages of a disruption; pre-disruption preparation, the disruptive event, and post-disruption (Madani & Parast, 2023). The *pre-disruption stage* is before the disruptive event has occurred when firms have already foreseen the event and can prepare, this stage can be extremely short. During this stage, a firm is already aware of the upcoming disruption. The second stage takes place *during the disruption*, it also involves the direct consequences and the preparation for recovery. The final *post-disruption stage* begins when the disruptive event is finished, and recovery plans are in place. The goal of achieving ER is to reduce the impact on performance following a disruption, to the fullest extent. Thus, reducing the drop in performance as seen in Figure 6 the most. This includes the desire to reduce the long-term impact or even overcome the disruption with a positive impact on performance over the shortest period.

To increase the ability of firms to deal with disruptions, and as a result, improve ER, Sanchis and Poler (2014) attempted to deliver a framework to categorize disruptions. Their framework is based on three steps: categorization of disruption sources, categorization of disruptive events, and categorization of consequences. By being able to identify a disruption and determine possible consequences and sources, firms are able to increase their preparedness for several types of disruptive events. This makes it an important manner in which a firm can deal with disruptions. While this framework proves highly suitable for the categorization of disruptions, enabling the identification of their sources and consequences, it lacks the provision of future remediation advice.

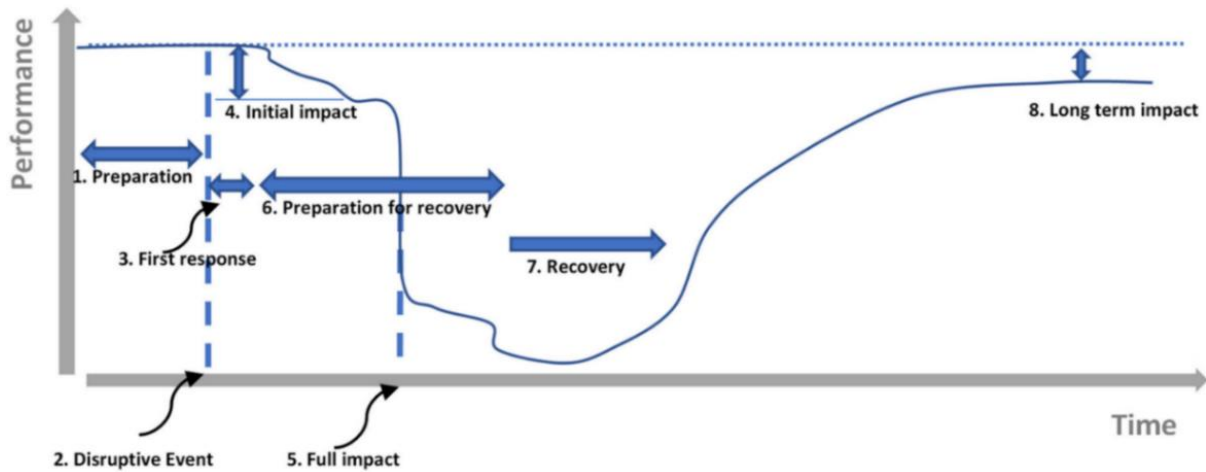


Figure 6: Disruption pattern (Madani & Parast, 2023)

### 3.2.1.3 Definition

In this section, various definitions of ER have been discussed, the necessary capabilities for ER have been identified, and disruptions have been examined more closely. Now, we synthesize this information into a single definition that is used for the remainder of this research:

*Enterprise Resilience is the capacity of an enterprise, to anticipate, respond to, and be prepared for disruptive events; and the ability to continuously recover, adapt, learn, and innovate from such an event in a way that the organization emerges from it strengthened and more resourceful.* (Hepfer & Lawrence, 2022; Sanchis et al., 2020; D. Wang & Chen, 2022)

Three definitions from the aforementioned authors were used to construct the definition for this report. They were chosen because they attempt to convey the same aspects concentrating on the proactive and reactive side of ER, as well as the ability to emerge strengthened from a disruption.

### 3.2.2 Information Systems Management

In the 1980's Keen (1980) identified requirements for making management information systems into a coherent research field. Currently, the field of information systems (IS) has matured into a recognized field of research. However, at the time, Keen (1980) suggested a set of questions for positioning management information systems (MIS) as a 'classical' research area. These questions focused on reference disciplines to MIS, how to build a cumulative tradition, the relation between MIS and computer technology, the relation to practice, a place to publish research on the topic, and the dependent variable. The *dependent variable* is used to measure success in IS research. DeLone and McLean (1992) attempted to define the dependent variable as a measure for information systems success. This resulted in the *DeLone & McLean model of IS success*, which consists of six interdependent dimensions of IS success, the model can be seen in Figure 7. It is noted there is not one success measure, but many. However, these measures all fall in one of the six dimensions of the model.



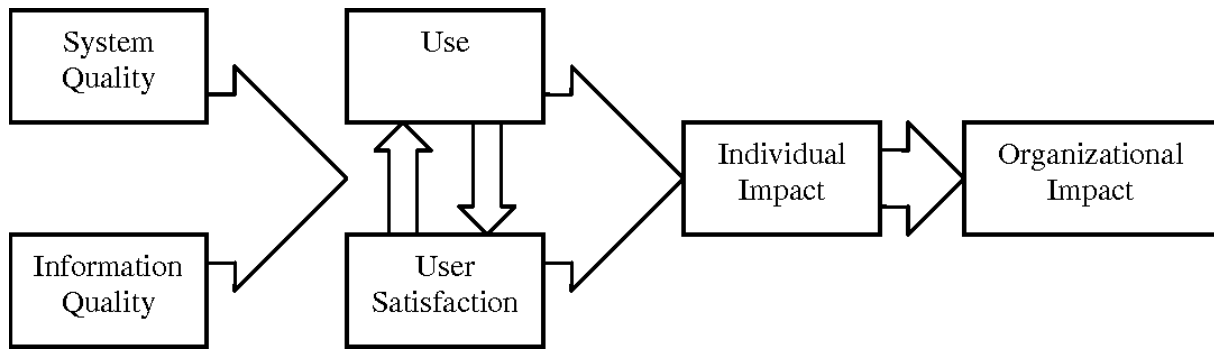


Figure 7: DeLone & McLean model of IS success (DeLone & McLean, 1992)

The model helped form a more concrete basis for the field of IS. Other researchers tried to extend the model, like Seddon (1997), who provided a clearer, more theoretically sound conceptualization of relationships between the various IS success constructs defined by DeLone and McLean. Seddon (1997) extended the model by clarifying the meaning of *IS use* and forming an extended model of IS use and IS success.

The relevant criticisms and suggestions towards the DeLone & McLean model of IS success over the years were apt reasons for DeLone & McLean to update their model (DeLone & McLean, 2003). The proposed extension by Seddon (1997) on IS use was taken into account as well as many other research contributions. From this, an updated IS success model followed. It includes additional arrows that show proposed associations among success dimensions in a process sense. However, it does not indicate whether these associations are positive or negative in a causal sense. For example, it is unclear whether high-quality IS corresponds with high net benefits and user satisfaction, and whether low-quality IS corresponds with dissatisfaction and negative net benefits. Furthermore, the addition of the *service quality dimension* was made. Because of the massive increase in end-use computing between the first iteration and the updated model, the inclusion of service quality is imperative, since the role of IS is not providing merely information anymore, but also providing a service. The updated model can be seen in Figure 8.

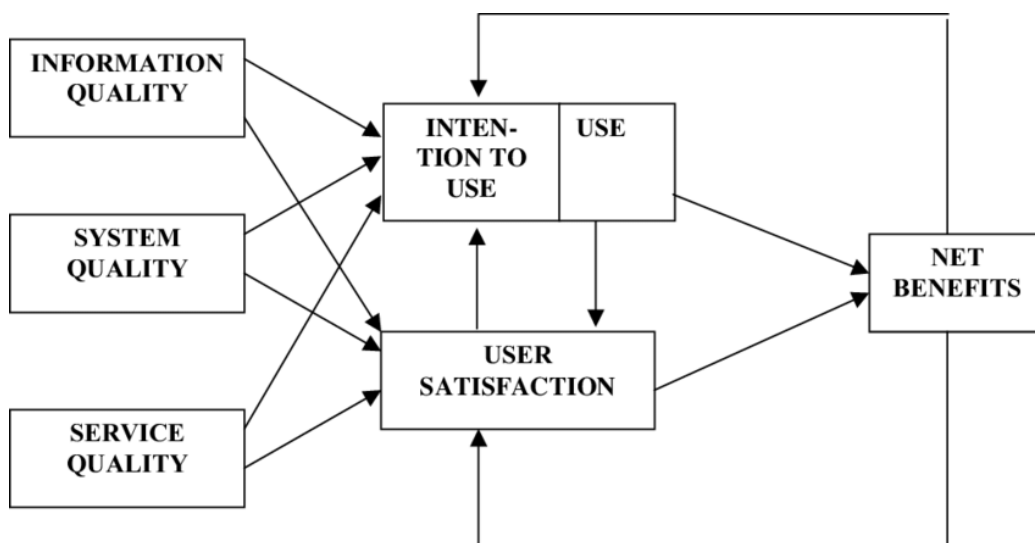


Figure 8: Updated DeLone & McLean model of IS success (DeLone & McLean, 2003)

Although continuous research in the field of IS causes it to evolve continuously, the model of IS success forms a firm theoretical basis for the field of IS and is still widely considered to be among the most influential theories in modern IS research, because thousands of scholarly articles have cited the IS success model to date (Al-Kofahi, Hassan, Mohamad, Intan, & Com, 2020). The theoretical background is followed by a more practical view of IS management.

A broad definition of an information system is *a system whose purpose is to process information* (Mallach, 2015). Five activities are included in processing information or data: *entering, processing, storage, sending, and using*. In a well-designed system, these activities are performed either by a device or a person that is purposefully assigned to that task. The inclusion of persons in ISs is crucial, even though IS is often merely related to technology. The inclusion of the usage dimensions (intention to use, use, user satisfaction) in the updated DeLone & McLean model also suggests persons are critical in IS (DeLone & McLean, 2003). Figure 9 shows a diagram that visualizes the components of IS; software, procedures, hardware, and people, all connected through data. The components below the centre are physically existing, the components above the centre instruct the corresponding elements on each side on what to do. Data, in the middle, is what holds the system together; the physical elements access data, and the elements that give instruction tell them what to do with it. Furthermore, the elements on the left of the diagram, together with data in the middle, are generally referred to as ‘information technology’ (IT); *IS involves people, IT does not*.

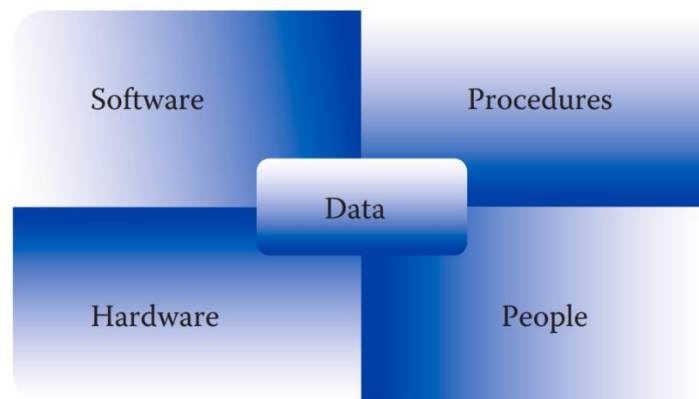


Figure 9: Conceptual diagram of IS (Mallach, 2015)

### 3.2.2.1 Definition

The remainder of this report utilizes the following definition of Information Systems Management:

*Information Systems Management is the usage of people and information technology and their relationships, for decision-making, coordination, and control within an organization.* (Mallach, 2015)

This definition formulated by Mallach (2015) is used for the rest of this report because it is a practical definition that concentrates on the relationship between people and information technology.

### 3.2.3 Risk Management

Risk Management can be defined as the identification, evaluation, and prioritization of risks followed by the application of resources to minimize, monitor, and control the impact of events

with a negative influence (Hubbard, 2020). In an attempt to provide a universally recognized paradigm for Risk Management, ISO31000 was published, wherein risk is defined as the *effect of uncertainty on objectives* (International Organization for Standardization, 2018). ISO31000 also defines the purpose of Risk Management as the *creation and protection of value*. Risk Management improves performance, encourages innovation, and supports the achievement of objectives.

Risk is increasing due to *globalization, technological complexity*, and an increased number of *interdependencies* (Rohmeyer & Zvi, 2009). Interdependencies occur in two ways: mutual dependencies between systems, also known as systems of systems, and the increasing dependencies of persons and institutions on IT. This implies managing this increased number of risks is becoming increasingly complex and requires additional attention. Risk Management became an exact science around the 1950s, mostly applied to finance and insurance. In the context of this review, Risk Management is not considered sector specific and is applied to organizations in general.

Firms that lack strategic risk understanding and foresight may expect to have trouble dealing with uncertainty. Therefore, some form of Risk Management is necessary to deal with these uncertainties originating from within the organization as well as from the external environment (Lisdiono et al., 2022). Risks can have an impact on the enterprise at various levels, such as internally on the resources (human and capital), the customers, or the products and services, and externally on society, markets, or the physical environment.

A popular approach to Risk Management is *enterprise risk management* (ERM), which is an overall risk management approach to business risks (D'arcy & Brogan, 2001). In ERM, the overall risks of the organization are managed in aggregate, rather than independently. It also considers certain risks as profit opportunities, which shifts decision-making from the level of insurance risk managers to the level of management, e.g., the board of directors. They would be more willing to embrace risk opportunities if profitability can be increased as a result. ERM has been shown to improve firm performance (Grace, Levery, Phillips, & Shimpi, 2015).

### 3.2.3.1 Risk Management strategies

Several strategies can be identified to manage risks. They can be classified into two categories: the deterministic approach, which includes quantitative, qualitative, and hybrid techniques, and the stochastic approach, which includes statistical approach and accident forecasting (Ennouri, 2013). In general, Risk Management strategies follow a similar process which consists of four steps (Tuncel & Alpan, 2010):

- *Risk identification*: The first step in Risk Management is the detection of any uncertain events that could negatively impact the organization.
- *Risk assessment*: Assessing the risk and identifying suitable actions to take is the next step. An assessment of risk can be made using the product of the probability of the event and the severity of the consequences occurring as a result of a risk. This product is often visualized in a risk matrix, as seen in Figure 10 (Ni, Chen, & Chen, 2010). The y-axis shows the severity of the consequences of an event, and the x-axis shows the probability of an event. Mapping risks on the matrix allows a user to rank the risks by their risk index, this can range from low to very high. Risks with a very high index need to be addressed first.

- *Risk Management*: The step in which action is taken, the suitable approach to managing the risk is chosen and implemented. Maximization of risk mitigation is key during this step.
- *Risk monitoring*: The efficiency of corrective actions needs to be measured. Also, in order to improve the holistic Risk Management system, potential future risk that has not yet been identified need to be uncovered.

Critical	M	M	H	H	VH	VH	VH
Serious	L	M	M	H	H	VH	VH
Moderate	L	L	M	M	H	H	VH
Minor	L	L	L	M	M	H	H
Negligible	L	L	L	L	M	M	H
Origin	0.00~0.10	0.10~0.20	0.20~0.40	0.40~0.60	0.60~0.80	0.80~0.90	0.90~1.00

Figure 10: Risk matrix (Ni et al., 2010)

Many different implementations of Risk Management lead to several frameworks that can be applied within an organization. When deciding on what Risk Management framework should be put in place, it is crucial to align it with the Risk Management initiative. A successful Risk Management framework is suggested to be: (1) *proportionate* to the present level of risk within a firm; (2) *aligned* with business activities; (3) *comprehensive, systematic, and structured*; (4) embedded within *business procedures and protocols*; (5) and *dynamic, iterative, and responsive to change*. This statement of principles identifies the essential features of Risk Management, on the other hand, a list of what Risk Management should deliver can be made. It should deliver: (1) mandatory *obligations* placed on the organization; (2) *assurance* regarding the management of considerable risks; (3) decisions that pay *full regard to risk considerations*; and (4) effective and efficient *core processes*. This set of deliverables, also known as MADE2, should be what a company is seeking to achieve when considering a Risk Management framework (Hopkin, 2018). Based on these distinctive lists covering what a successful Risk Management framework should be and what it should deliver, an enterprise can make an appropriate choice concerning a Risk Management framework.

### 3.2.3.2 Definition

The remainder of this report utilizes the following definition of Risk Management:

*Risk Management is the identification, evaluation, and prioritization of risks followed by the application of resources to minimize, monitor, and control the effects of uncertainty on objectives.* (Hubbard, 2020; International Organization for Standardization, 2018)

This definition was constructed to extend the definition by Hubbard (2020) to a more complete form that covers the definition of risk as well.

## 3.3 Information Systems Management & Enterprise Resilience

This chapter attempts to answer RQ1.1; *What is Information Systems Management and how does it relate to Enterprise Resilience?* As discussed in section **Fout! Verwijzingsbron niet**

**gevonden.**, the field of Information Systems Management at this point is considered mature, however, research on its relation and impact on ER is still rudimentary, as mentioned in section 3.1.1. Thus, this section presents a review of the available literature on the relationship between Information Systems Management and ER. The usage of information systems offers a lot of value to firms, however, with this also comes certain risks due to the increased complexity and interdependence that accompanies Information Systems Management. It is, therefore, crucial to consider the usage of IS in a value-creating light towards ER, while also highlighting the risks and upholding the unbiased view necessary for an SLR.

Before any alignment between Information Systems Management and Risk Management with the goal of ER can even be considered, the link between Information Systems Management and ER needs to be examined. Attempts at conceptualizing this link have been made in the literature. Heeks and Ospina (2019) mention that a lot of research discussing Information Systems Management and ER concentrates on 'resilience of information systems'. The focus, in the work of Heeks and Ospina (2019), is not on the impact of ISs on company-wide ER, but on the level of resilience of an IS or IS infrastructure. RQ1.1 is not concerned with this relationship, instead, the interest is on what Heeks and Ospina (2019) call '*resilience of an information system outcome system*'. Which they define as the research that considers the impact of IS on the resilience of other, wider systems that the IS supports. They mention little research has been done on this concept as of 2019.

Erol et al. (2010) attempted to conceptualize this relation which resulted in a framework that proposes two key enablers of ER; *enterprise architecture* (EA) and *enterprise integration*. It was found that an enabler of ER was the alignment of information technology and business goals. Such an alignment requires modelling the underlying technology infrastructure and its usage and capturing this in a consolidated view. To achieve this, they argue for enterprise architecture as an appropriate tool, since it can be used to model and provide a simplified and well-defined view of all available resources and enables the *alignment of business and technology*. It should be noted that enterprise architecture encompasses the entire firm, so Erol et al. (2010) do not solely argue for IS as an enabler for ER, but for the alignment with business goals as an enabler for ER. Gomes (2015) also argues for EA as a way to make ER more predictable and achievable in SMEs.

Earlier research was performed by Ignatiadis and Nandhakumar (2007) on the impact of enterprise systems, specifically enterprise resource planning systems (ERP), on ER. Where they define an enterprise system as a tool to facilitate seamless integration and exchange of data between different departments within a firm. However, although the study focused on ERPs, they state the results can be applied to other enterprise-wide information systems. They found the use of enterprise systems can positively influence the level of ER. It is argued that enterprise systems increase *decentralization of decision-making*, while also making possible *centralization of control and knowledge* (Orlikowski, 1991). Decentralization of decision-making may increase the resilience of an enterprise by relaxing centralized control and rigidity, which promotes flexibility. However, centralization of control and knowledge can decrease ER if not managed correctly, since dependence on departments with high control and centralization can lead to an imbalance between departments.

A study by Velu et al. (2019) examined the effect of the usage of IS artefacts on ER. The direct effect was measured; however, in addition, the IS artefact was also considered as a mediating aspect between ER and a set of proposed organizational capacities. More specifically, they considered the collective perception of employees towards these capacities and their impact

on the IS artefact. So, they investigated whether employees' views towards capacities like commitment, communication, community, competency, connection, and coordination have a significant effect on the IS artefact. They found a significant relationship between the capacities and the IS artefact. This means, for example, a positive perception of community within the company positively affects the IS artefact since it enables collaboration through the usage of the IS artefact. The authors concluded that positively combining the capacities leads to increased IS artefact usage, which in turn was found to lead to increased ER. Their conclusion supports the assumption that *combining people equipped with the right capacities* with IS artefacts enables organizations to become more resilient (Mallak & Yildiz, 2016).

Flexibility and agility have been mentioned as enabling characteristics to achieve ER (Conz & Magnani, 2020; Erol et al., 2010; Heeks & Ospina, 2019; Madani & Parast, 2023). These are also mentioned by Ciampi et al. (2018) as resulting factors from using *big data analytics capable information systems*. Big data analytics capable information systems span the whole organization and can collect an enormous quantity of data collected from analysing business processes in real-time. These systems are a combination of traditional ISs and *artificial intelligence* (AI) capabilities, which allow machines to automatically learn from data and make meaningful decisions without human interference. They argue that because of this, big data analytics capable information systems provide an opportunity for businesses to *increase strategic flexibility and agility*, leading to increased ER. Opposed to traditional ISs, big data analytics capable information systems can adapt themselves to different kinds of data, which allows them to provide organizations with markers of change arising in any environment (Thiede et al., 2018). By applying new technologies like big data analytics and AI, Ciampi et al. (2018) argue that increased ER can be achieved due to increased flexibility and agility, a similar conclusion was drawn by Schemmer et al. (2021) who argue for the use of AI-based IS to increase resilience. Although the usage of new technologies can have many upsides, they are also accompanied by many risks. Decision-making by AIs reduces the visibility of the process due to the 'black box' that such AI systems come with. The 'black box' is where the internal logic and operations of such a system happen, which is not observable. This means putting a lot of trust in an AI system which is associated with risk.

Furthermore, D. Wang and Chen (2022) discuss the positive effects of *digital transformation* on ER, where digital transformation concerns technologies like AI, big data analytics, cloud computing, and blockchain. They found the application of these technologies can improve ER by improving the level of human capital, enhancing innovation capabilities, easing credit constraints, and strengthening internal control.

Although usage of IS is not always related to increased resilience due to the risks that come with complex IS infrastructures, there is also proof to be found in the literature that argues that properly managed IS supported by the right capacities can lead to increased ER. Alignment between business and technology through EA is mentioned as an enabler for ER. Furthermore, decentralization of decision-making is a result of IS usage, which relaxes centralized control which leads to flexibility, an enabler for ER. Moreover, strong relations between ER and the usage of new, flexible technologies like big data analytics and AI have been identified. The main findings concerning RQ1.1 can be found in Table 8.

*Table 8: Main findings RQ1.1*

<b>Main findings RQ1.1</b>
----------------------------



A strong alignment between information technology and business goals can be achieved by enterprise architecture. Thus, through enterprise architecture, firms have better insights into their implementation of information technology concerning their business goals, which makes it more achievable through increased visibility to improve Enterprise Resilience. (Erol et al., 2010; Gomes, 2015)

The use of enterprise systems (enterprise-wide information systems) can positively influence the level of Enterprise Resilience. It is argued that enterprise systems increase decentralization of decision-making, which may increase the resilience of an enterprise by relaxing centralized control and rigidity, which promotes flexibility. (Ignatiadis & Nandhakumar, 2007; Orlikowski, 1991)

The usage of an IS artefact has a positive effect on Enterprise Resilience when it is supported by the correct capabilities: commitment, communication, community, competency, connection, and coordination. Suggesting that when you have people equipped with the right capabilities, an IS artefact has a positive effect on increasing Enterprise Resilience. (Mallak & Yildiz, 2016; Velu et al., 2019)

Big data analytics capable information systems supported by AI capabilities can make decisions based on datasets too large for humans to comprehend and can adapt to changes in the data. Because of this, they provide an opportunity for businesses to increase strategic flexibility and agility, as well as monitor changes in the environment which can point to disruptions. Having access to these tools leads to increased ER. (Ciampi et al., 2018; Thiede et al., 2018)

### 3.4 Risk Management & Enterprise Resilience

In this chapter, the collected literature is used to answer RQ1.2: *What is Risk Management and how does it relate to Enterprise Resilience?* An examination of the relationship between the topics is presented similar to the process used for RQ1 in section 3.3. So, before alignment can be considered, the individual impact from both fields on ER needs to be considered.

In today's turbulent business environment, firms are facing steeper competitive pressure, they must deal with rapidly changing technologies and resource scarcity, also, they are expected to find more sustainable ways to develop their organization. Because of this, firms must go beyond traditional approaches to Risk Management (Assibi, 2022). In this rapidly changing operating environment, *Risk Management and resilience strategies* are emerging as keystones to success. Assibi (2022) mentions implementing such a strategy requires a broader range of tools compared to traditional Risk Management, to identify what risks are most critical to their future performance. Based on this, proactive steps should be taken to optimize ER. Other studies have also empirically studied and found a positive relationship between Risk Management and ER (Hudakova & Lahuta, 2020; Lisdiono et al., 2022).

The goal of RQ1.2 is to examine the impact of Risk Management on ER. However, Pettit et al. (2014) interpret this relation differently. Although they acknowledge that improved ER can follow from high-level Risk Management, they also mention that Risk Management and the concept of resilience can be applied to different situations. As visualized in Figure 11, when one is dealing with a stable system only impacted by known risks, probabilistic Risk Management is sufficient. However, in a volatile system faced with unknown risks, inherent resilience is necessary. But since risk, as discussed in section **Fout! Verwijzingsbron niet gevonden.**, is becoming increasingly unknown and the general business environment is becoming more volatile (Rohmeyer & Zvi, 2009), most firms find themselves in the top-right

quadrant. This implies that companies will benefit from increasing their level of ER and probabilistic Risk Management is not sufficient anymore by itself.

Volatile system	Learning and adaptation	Inherent resilience
	Probabilistic risk management	Detection and response
	Known risks	Unknown risks

*Figure 11: Appropriate strategies for different operating conditions (Pettit et al., 2014)*

The alignment between Risk Management and *business continuity management* (BCM) is mentioned as a contributor to the creation of ER (Bukanová et al., 2021; Teoh & Zadeh, 2013). BCM is a management process that is concerned with identifying potential threats and their impact on the day-to-day operations of a firm, with the goal of *maintaining business functions*. It incorporates elements from disaster planning and crisis management. However, Taylor (2014) argues that BCM is commonly implemented as a short-term survival response, but this by itself does not lead to ER. To achieve ER, longer-term responses should be implemented with the goal of *not just surviving but thriving* in the long term. But Bukanová et al. (2021) argue that aligning BCM and Risk Management strategies can lead to increased ER, through a focus on continuous monitoring of activities, a bigger emphasis on prevention, planning, and preparedness, and improvement to crisis response.

Rohmeyer and Zvi (2009) mention that the output of the ERM process should be a *resiliency management program*. The goal of such a program should be to attempt to identify all threats specifically to resiliency, based on the unique risk environment of a firm. Especially since risk environments across all sectors are changing and becoming more volatile and complex (Schinagl et al., 2023). A dedicated resiliency management program should be *interwoven with the strategic objectives* of a firm, instead of a separate support program. A separate support program is generally the attempted solution for improving resilience. In a practical sense, a resiliency management program is an overview that presents a control point for each enumerated risk. Each risk should be analysed regarding the respective vulnerabilities, the impact of the risk event, and the likelihood of occurrence. Followed by the design of an appropriate mitigation strategy for each risk. Monitoring and testing of each mitigation strategy should be scheduled as well. The concept of a resiliency management program shows the acceptance of Risk Management practices in attempts at improving ER.

Oh and Teo (2009) also examined the relationship between ERM and resilience. Specifically, regarding capabilities necessary for ERM. They identify these capabilities as *risk measurement, risk control, and risk monitoring*. They extended these capabilities by including the usage of IT, also known as *IT-enabled ERM capabilities*. These are conceptualized as the ERM capabilities expanded with the use of data and analytics. Their findings show a significant impact of IT-enabled ERM capabilities on ER since organizations with strong IT-enabled ERM



capabilities can detect threats further in advance and assess their impacts quickly. Capturing this critical information early and accurately, allows firms to *anticipate potential disruptions at an earlier level* than organizations whose IT-enabled ERM capabilities are immature. It also provides a variety of responses to threats based on for example historical data. As a result, organizations are able to minimize the negative effects of disruptions and continue normal operations in a reduced amount of time. It should be noted that IT-enabled ERM capabilities have a slightly weakened effect on ER for firms with access to a strong network structure. These firms can rely more on external information advantages and other resources from their network.

Skulimowski and Łydek (2022) took the usage of data and analytics even further in their approach to Risk Management to achieve resilience. They propose a *Risk Management decision support system aligned with AI principles* to achieve long-term Risk Management and resilience building. A decision support system for Risk Management that incorporates techniques like machine learning of threat models, sensor information fusion and understanding, and multicriteria decision-making procedures, is capable of *recommending situation-dependent risk mitigation actions and long-term strategic resilience building*. Previously, systems have been used to provide, visualize, and present data to decision-makers, however, an AI-aligned Risk Management decision support system can be capable of solving heterogeneous industrial threat management problems by itself without human interference. According to Skulimowski and Łydek (2022), this leads to long-term resilience building.

Researchers have taken different views towards the relationship between Risk Management and ER. Some consider Risk Management as an inherent part of ER; others mention that Risk Management and improved ER are concepts that can be applied to different situations. However, many also mention the positive impact Risk Management can have on ER. This can be achieved through the alignment with other strategies, like BCM. Or the application of ERM strategies to generate a resiliency management program, that considers each enumerated risk to achieve ER. Combining Risk Management with technologies is also discussed, for example, extending ERM capabilities by making them IT-enabled. It might even be possible to go beyond this by applying new technologies like implementing a Risk Management decision support system aligned with AI principles. Overall, a strong relationship between Risk Management and ER can be observed in the literature. Different interpretations are present, but a positively impactful relationship can be observed. The main findings concerning RQ1.2 can be seen in Table 9.

*Table 9: Main findings RQ1.2*

#### **Main findings RQ1.2**

By combining Risk Management strategies and business continuity management strategies, Enterprise Resilience can be improved. Business continuity management is often a short-term survival response, which does not directly contribute to Enterprise Resilience. By combining it with Risk Management, long-term strategies can be implemented that improve Enterprise Resilience. (Buganová et al., 2021; Teoh & Zadeh, 2013)

Enterprise risk management is a Risk Management strategy that can be used to create a resiliency management program. This should serve as a dedicated strategy interwoven with strategic objectives, instead of it being a separate support program. By incorporating Risk Management strategies at this level within a firm, Enterprise Resilience can be improved. (Rohmeyer & Zvi, 2009)

Capabilities necessary for enterprise risk management are risk measurement, risk control, and risk monitoring. By supporting these capabilities with IT, through the usage of data analytics, threats can be detected further in advance and their impact can be assessed quickly. Early detection and assessment of these threats allow firms to proactively minimize the negative effect of disruptions. (Oh & Teo, 2009)

The usage of data and analytics can be taken further using AI principles. Risk Management support systems are enabled by AI, through technologies like machine learning of threat models, sensor information fusion and understanding, and multicriteria decision-making procedures. Using these technologies, such a system can provide situation-dependent risk mitigation actions as well as long-term strategic resilience building. Improving the overall level of Enterprise Resilience of a firm. (Skulimowski & Lydek, 2022)

## 3.5 Discussion

This chapter first defines the topics of Information Systems Management, Risk Management, and Enterprise Resilience separately based on relevant and recent literature. This is followed by a closer examination of the relationships between Information Systems Management and Enterprise Resilience, and Risk Management and Enterprise Resilience.

RQ1.1 is concerned with Information Systems Management and its relationship to Enterprise Resilience: *What is Information Systems Management and how does it relate to Enterprise Resilience?* Various definitions across the literature led to the following definition for Information Systems Management: *Information Systems Management is the usage of people and information technology and their relationships, for decision-making, coordination, and control within an organization* (section 3.2.1.3). Due to the increased complexity introduced by the implementation of information systems, ISs are occasionally associated with the introduction of disruptions, however, a positive relationship between Information Systems Management and Enterprise Resilience can be identified (section 3.3). This positive effect on Enterprise Resilience can only be achieved by proper Information Systems Management supported by the right capabilities. The use of enterprise architecture has been mentioned to support this. Another relationship that can be identified is increased flexibility through IS usage, which is an enabler for Enterprise Resilience. And lately, the development in Information Systems Management through new technologies has been mentioned as an enabler. Technologies like big data analytics and AI are examples of this (Main findings in Table 8).

The relationship between Risk Management and Information Systems Management was examined to answer RQ1.2: *What is Risk Management and how does it relate to Enterprise Resilience?* The available literature was used to define Risk Management as follows: *Risk Management is the identification, evaluation, and prioritization of risks followed by the application of resources to minimize, monitor, and control the effects of uncertainty on objectives* (section 3.2.3.2). An inherent relationship between Risk Management and Enterprise Resilience is often mentioned, Risk Management is a part of achieving Enterprise Resilience according to many, which implies a positive effect (section 3.4). Risk Management

is often mentioned as an enabler for Enterprise Resilience in combination with other strategies, like business continuity management. A method to use Risk Management is the creation of a resiliency management program which lends concepts from enterprise Risk Management. Technology usage is also mentioned. Lately, new technologies like Risk Management decision support systems using AI principles are proposed as powerful support tools for Risk Management to increase Enterprise Resilience (Main findings in Table 9).

The main contribution of this chapter is the identification of overlap between the relationships mentioned in the research questions. IT-enabled enterprise risk management capabilities have been found to positively influence enterprise risk management. Traditional Risk Management is combined with the usage of IT. For example, by using data analytics to support risk assessment, threats can be identified further in advance. This can be extended by newer technologies that allow for more advanced usages of data. The increasing amount of produced data by companies results in what we call big data. Examining big data can reveal novel, meaningful findings that were previously unattainable due to less advanced technology. The introduction of AI in this process can even automatize this to an extent, and it can even be used to support high-level decision-making regarding Risk Management in a firm. These are initial findings that provide directions for how enterprises must arrange their Information Systems Management and Risk Management activities to actively work towards improved resilience. The inclusion of data analytics in the construction of ER remains a relatively novel concept, therefore, potentially posing complexities in its integration into the resultant methodology of this research.

However, these findings are general points of attention that combine Information Systems Management and Risk Management to achieve increased Enterprise Resilience. Enterprises cannot practically (re-)arrange their Information Systems Management and Risk Management structures based on these findings alone. Detailed insights into the exact requirements to do so are missing, and a practical method that instructs enterprises on these points is lacking.

# 4 Requirements Analysis & Methodological Considerations

---

Chapter 4 covers the requirements for the design of the method, as well as further methodological considerations related to the design choices and the used instruments. The requirements to which the final method must adhere are first introduced and motivated in section 4.1, requirements are only valid if they contribute to a goal of a relevant stakeholder. The guidelines along which the method is designed are described in section 4.2. The literature on which the initial artefact was based is described, as well as the design choices that were made for the structure of the method. Also, the modelling language that is used to visualize the method is introduced in section 4.3. Thereafter, the validation plan is described. Two main instruments are utilized; validation through expert opinions, and applying the method to an existing case.

## 4.1 Requirements

Specifying requirements is an essential part of the design science methodology by Wieringa (2014). Because requirements describe the desired properties of a system based on the desires of the relevant stakeholders. Formulating the requirements based on stakeholder desires ensures the system only exhibits behaviours that create value for the stakeholders and ensure no useless properties are implemented. For this reason, a designer must provide a contribution argument for each requirement. A contribution argument justifies the choice for some requirement by defining what the requirement, in an assumed context, will contribute to a stakeholder goal.

For this research, two types of requirements for the artefact are specified; functional- and non-functional requirements. Functional requirements describe what an artefact must do, and what its functions and features are. It is generally a straightforward process to assess whether a functional requirement was met since one can simply test whether the required functionality is available.

The other type is the non-functional requirements. Non-functional requirements are global properties of the interaction between the artefact and its context. It describes how the system goes about delivering a specific function. In short, it describes how the system works. So, non-functional requirements do not have any impact on the functionality of the artefact, but they do impact its performance. One way to differentiate functional and non-functional requirements is that functional requirements ensure a working artefact is delivered. Technically speaking, the artefact could reach a working state while ignoring the non-functional requirements. However, in practice, it would not meet many user expectations and performance would most likely be very low. Thus, to ensure a functional system that is also practical, both functional- and non-functional requirements are specified.

The properties of the artefact described by non-functional requirements need to be operationalized to test their presence. Often, one cannot test these properties because no norm exists for them. To operationalize the desired properties, indicators must be defined. Indicators are variables that can be measured and that indicate the presence of the property.

The following sections describe the functional- and non-functional requirements of the artefact, as well as their contributions to stakeholder goals, and the indicators for non-functional requirements.

### 4.1.1 Functional requirements

The following section describes the functional requirements the method must comply with. They are described and additionally, the reasoning for their existence is mentioned. They are outlined in Table 10 below.

*Table 10: List of functional requirements*

	<b>Functional requirement</b>	<b>Reasoning</b>
F1	Method must be implemented at the strategic level of a firm	As mentioned in section 1.2 on the research scope, ER is a capacity that spans the whole organization. Therefore, a method that attempts to improve it, must be implemented at the level that can impact the whole organization, which is the strategic level. This assessment followed from the SLR (section 3.2.1).
F2	Defines how the IT department must behave at a strategic level	From the stakeholder analysis, it followed that resources were lacking that describe how ER can be achieved by aligning ISM and RM. Therefore, it follows that a method that attempts this must provide direction on how the IT department and risk managers must behave at the strategic level.
F3	Defines how IT department processes must be structured	Similarly to the reasoning for F2, the method must describe how the main processes executed by the IT department or risk managers that could influence ER must be structured.
F4	Defines how risk managers must behave at a strategic level	See F2.
F5	Defines how Risk Management processes must be structured	See F3.
F6	Defines how collaboration between IT department processes and Risk Management processes should be arranged	The objective of the method is to align ISM and RM. This involves collaboration between the risk managers and the IT department. Therefore, in addition to providing instruction for each separately, the method must outline the collaboration between them.
F7	Introduces holistic risk awareness across the enterprise	Holistic risk awareness was observed from the literature as being an essential quality for achieving ER. A method that is implemented at the strategic level will affect lower levels, therefore, a holistic risk awareness across the organization is crucial to instilling the right mentality for increasing ER.

F8	Data-driven approach, utilizing AI and BDA, allows new insights	One of the main findings (Section 3.5) from the SLR was the positive effects of data-driven solutions on ER through both ISM and RM. So, it must be included in the method.
----	---	---

Next, contribution arguments are given that define what the impact of implementing the requirement aspects contribute towards stakeholder goals, that were defined in section 1.3. F1 aims at ensuring the method is applied at the level that impacts ER, which is the strategic level. This contributes to the goal of the client firms to be able to anticipate and react to disruptions which together leads to increased ER.

F2, F3, F4, F5, and F6 are all of the same nature and all contribute to the same stakeholder goal, since all involved stakeholder profit from practical instructions that enhance ER. They are all looking for resources that provide ER enhancement, and that is exactly what these five requirements ensure.

F7 aims at ensuring the introduction of holistic risk awareness, which should lead to an enterprise-wide understanding of the relevancy of adopting the method. This contributes to the goal of client firms of business continuity since the adoption of a new method can be a source of disruption. Which would lead to the opposite of the desired effect of mitigating disruptions.

Finally, F8 contributes to the goal of KPMG ITA management. A method that allows leveraging the latest technologies that client firms may be unfamiliar with, improves the service quality that KPMG can offer by opening new doors to their clients.

### 4.1.2 Non-functional requirements

This section describes the non-functional requirements as seen in Table 11. Alongside the requirements and the reasoning for their existence, indicators are given that serve to operationalize the non-functional requirements, this allows them to be validated. They are given in Table 12.

*Table 11: List of non-functional requirements*

	Non-functional requirement	Reasoning
NF1	Must be scalable with the risk environment the firm finds itself in	As mentioned in section 3.4 on RM and its relation to ER, risk environments across all sectors and firm sizes are changing and becoming increasingly complex and volatile. This means an increased level of ER benefits firms that face different levels of risk since likely all will be facing increased risks at some moment in time. Therefore, the method must be applicable to firms that find themselves in various risk environments.
NF2	Must be practically implementable and usable	While defining the design problem (section 2.1.1), it was concluded that most available treatments are largely conceptual in nature and do not provide many practical steps to enhance ER. Therefore, this method must fill this gap by focusing on practical applicability and clear to users.

NF3	Must be compatible with current operations, it must fit on top of any current framework or method	As mentioned in the research scope (section 1.2), implementing the method must not disturb the operations of the firm or force any massive changes in governance like abandoning a framework that is currently implemented in the firm. Instead, the method must fit on top of any current governance frameworks.
NF4	Must be an iterative method that aims at continuous ER improvement	A critical part of ER is 'bouncing forward' after recovering from a disruption as mentioned in the SLR (section 3.2.1). Therefore, the method must provide a way to ensure a continued focus on improvement, which can be accomplished by designing a method that iteratively can be followed.
NF5	Must encourage long-term growth	Achieving ER is not the same as surviving the disruptions. The goal is to grow into a more resilient organization as was one of the findings from section 3.4 on RM and ER. So, the method must aim at achieving long-term growth.
NF6	Promotes distributed autonomy for departments	Decentralization of decision-making increases flexibility and adaptability in times of crisis as mentioned in section 3.3 on ISM and ER. Therefore, the decision-making structure must not strictly be top-down, instead, space must be created for distributed autonomy.

NF1 does not specifically contribute to one of the mentioned goals of the stakeholders. Since this requirement follows from the scope that was set for this research, and thus contributes to one of the overarching goals of this research instead. This goal is to design a method that is not focused on a specific type or level of risk, but instead provides a course of action for many different risk environments.

A practical method must be applied to effectively increase ER, therefore, NF2 contributes to increasing preparedness for disruptions and a better reaction to disruptions for the client firm. Similarly, the adoption of the method must be a feasible process. NF3 contributes to this by ensuring that the adoption itself is not disruptive.

As described in the reasoning for NF4, 'bouncing forward' is a critical part of building ER. By fulfilling NF4, continuous improvement can be achieved which contributes to increased ER at the client firm. In a similar sense, NF5 ensures that the method is not used as a temporary tool for solving a crisis. Instead, the method aims at interweaving an awareness of ER into the organization.

A specific department has the most knowledge of the risk and disruptions they might face. Therefore, the method must not take away the autonomy of a department when it comes to this as described in NF6.



*Table 12: List of non-functional requirements and indicators*

	<b>Non-functional requirement</b>	<b>Indicator</b>
NF1	Must be scalable with the risk environment the firm finds itself in	Expert opinion must be positive on the effectiveness of artefact in lower vs. higher risk environment
NF2	Must be practically implementable	Expert opinion must be positive on the feasibility of practical adoption
NF3	Must be compatible with current operations, it must fit on top of any current framework or method	The method must not require any immediate change to an established framework or method
NF4	Must be an iterative method that aims at continuous ER improvement	The method must have a component that ensures iteratively.
NF5	Must encourage long-term growth	Expert on opinion must be positive on the long-term effectiveness of the activities specified in the method.
NF6	Promotes distributed autonomy for departments	No activities specified in the method must force any enterprise-wide rules that must be adhered to.

Table 12 lists all non-functional requirements, accompanied by an indicator that operationalizes the requirement. Defining these allows the non-functional requirements to be validated. Because this research does not cover the treatment implementation phase (see section 2.1) of the design cycle by Wieringa (2014), some non-functional requirements can only be validated through expert opinion. Preferably they would be tested in an environment where the artefact is implemented, however, due to the scope of the research this is not feasible.

## 4.2 Design Approach

The design of the method is based on data collected from the literature and expert opinions through semi-structured interviews. These sources can be considered reliable sources of information if appropriately used, which is the case when the interviews are objectively processed and the results purely reflect the thinking of the interviewees. The involvement of the experts occurs after an initial version of the method has been established that is designed based on findings from literature and alternative treatments, these findings are described and motivated in section 4.2.1. This initial version will be incomplete, it mostly serves as a basis which is extended through multiple iterations of the design cycle. Most importantly, the design choices that give structure to the method described in section 4.2.2 are validated during the first round of interviews. These design choices describe the different dimensions on which the method was built.

The method was designed using the modelling language ArchiMate. This language is introduced in section 4.2.3, the relevant aspects of the language are explained so the method can be understood to the fullest extent.



## 4.2.1 Design of initial artefact

This section describes the aspects that were identified in the literature as contributors to ER, together these aspects form the basis for the initial method. Since no treatments currently exist for the research problem presented in section 2.1.1, the identified aspects are separated into two separate categories similar to those used during the SLR. A distinction is made between Risk Management aspects that lead to ER, and Information Systems Management aspects that lead to ER. Aspects in this context refer to business processes and functions that may be suitable for alignment.

All identified aspects originate from either the SLR or from alternative treatments found through an exploratory review. This exploratory review was focused on finding more practically-aimed solutions to the design problem since results from the SLR are generally more conceptual. The design problem was once more split up into Information Systems Management aspects and Risk Management aspects since an aligned method is not yet available.

The identified Risk Management aspects that lead to increased ER are presented in Table 13. Information Systems Management aspects leading to increased ER are presented in Table 14.

*Table 13: Risk Management aspects leading to ER*

<b>Risk Management aspects</b>	<b>Description</b>
Federated Risk Management approach (GRC 20/20 Research, 2022)	A balanced approach between departmental autonomy and common governance across departments regarding Risk Management, allows for control across common risk relationships while allowing different departments to focus on their specific risk areas.
Risk and resilience management process architecture (GRC 20/20 Research, 2022; Oh & Teo, 2009)	<p>Adapting the established Risk Management process to install a resilience-aware culture:</p> <ul style="list-style-type: none"> <li>- Identification of objective, process and service               <ul style="list-style-type: none"> <li>o Identify at strategic level to get overview of relevant risk environment</li> </ul> </li> <li>- Establish impact tolerances               <ul style="list-style-type: none"> <li>o Definition of what the level of impact of risks from objectives, processes, and services can be tolerated</li> </ul> </li> <li>- Risk identification</li> <li>- Risk assessment               <ul style="list-style-type: none"> <li>o Define point solutions to purpose-built for very specific risk and regulatory issues that the organization can expect to face at some point</li> </ul> </li> <li>- Risk treatment               <ul style="list-style-type: none"> <li>o Consider business continuity management and set up response and disaster recovery plans</li> </ul> </li> <li>- Risk and resilience monitoring               <ul style="list-style-type: none"> <li>o Contributes to 'bouncing forward'</li> </ul> </li> <li>- Risk and resilience communication &amp; attestations               <ul style="list-style-type: none"> <li>o Contributes to 'bouncing forward'</li> </ul> </li> </ul>

<p>Reactive ability to fulfil major objectives to stakeholders (Louisot, 2015)</p>	<p>Maintaining the ability to fulfil major objectives to crucial stakeholders is a priority in recovery from a disruption:</p> <ul style="list-style-type: none"> <li>- Stockholders; maintain profitability &amp; dividends</li> <li>- Personnel; retain employment levels &amp; pays salaries</li> <li>- Economic partner; secure contractual terms and conditions</li> <li>- Society; comply with laws and regulations</li> </ul>
<p>The right answer to different levels of disruption (Louisot, 2015)</p>	<p>Properly labelling disruption is crucial. Labelling everything as a crisis creates a crazing effect that could generate a crisis or an indifferent attitude from staff that will not react when a real crisis occurs.</p> <p>On the continuous disruption level following states could be used:</p> <ul style="list-style-type: none"> <li>- Simple state; it is the state for which the system has been set up. Stability; clear cause/effect relationships</li> <li>- Complicated state; where expertise is essential and the domain of 'good practices'. In which operational managers and risk owners can handle daily variations</li> <li>- Complex state; where innovating solutions must be investigated ahead of the situation to plan for action, where business continuity plans are an efficient tool</li> <li>- State of chaos or rupture; when acting fast is essential but with a strategic vision that is beyond operational managers and require the input of top management. The level of disruption that calls for strategic redeployment planning</li> </ul>
<p>Knowledge registration actions (Sanchis et al., 2020)</p>	<p>Keep a detailed register of disruptions to create knowledge basis which supports growth by learning from previous disruptions. The following information should be registered:</p> <ul style="list-style-type: none"> <li>- Disruption event: Name, Date, Time, Description, functional areas or departments involved, staff involved, causes identified (if any), Legislative/regulatory aspects, Short-term consequences, Long-term consequences</li> <li>- Historical Registration: Protocol number (if available), Number of times the disruptive event has already happened, Preventive actions that have already been implemented (if any), Previous experiences in the recovery of this disruptive event)</li> <li>- Recovery actions: Description, steps, people involved, responsible, time, duration, remarks, actions suitability</li> </ul>

Risk and resilience management team (GRC 20/20 Research, 2022)	The first piece of the strategic plan is building the cross-organization Risk Management team (e.g., committee, group) or position. This team needs to work with risk owners to ensure a collaborative and efficient risk governance process is in place. The goal of this group is to take the varying parts of the organization that have a vested stake in Risk Management and gets them collaborating and working together on a regular basis.
--	--

*Table 14: Information Systems Management aspects leading to ER*

<b>Information Systems Management aspects</b>	<b>Description</b>
Usage of centralized risk and resilience management platform (GRC 20/20 Research, 2022)	Departmental autonomy concerning Risk Management is encouraged, but a centralized risk and resilience management platform provides an overview of the complete risk environment and a central hub for overall analysis and reporting to support risk-intelligent decision-making.
Reprioritize for resilience (KPMG, 2020)	Review planned changes and reprioritize for resilience, capacity, and performance improvements and limit non-critical changes to the IT estate.
Proactive resilience building in IS (short-term building) (KPMG, 2020)	<p>To build resilience in IS short term, the following aspects must be reviewed for their contribution towards resilience:</p> <ul style="list-style-type: none"> <li>- IT governance, risk, and control <ul style="list-style-type: none"> <li>o Ensure controls work correctly and IT governance is aligned with increasing Enterprise Resilience</li> </ul> </li> <li>- IT priorities <ul style="list-style-type: none"> <li>o For rapid adjustment and flexibility</li> </ul> </li> <li>- Data security</li> <li>- Data centre recovery process</li> <li>- Uninterruptible power supply</li> </ul>

<p>Reactive resilience building in IS (long-term building) (KPMG, 2020; Xu, Tsang, Chew, Siclari, &amp; Kaul, 2019)</p>	<p>To build resilience in IS long term, the following activities may be executed:</p> <ul style="list-style-type: none"> <li>- Apply lessons learned from disruption to adjust the IT operating model as business returns to equilibrium</li> <li>- Review underlying risk and IT frameworks</li> <li>- Review and reprioritise strategic technology investments and accelerate programs that support resilience building</li> <li>- Review sourcing of hardware</li> </ul>
<p>Intelligent automated technologies (Ciampi et al., 2018; KPMG, 2020; Skulimowski &amp; Łydek, 2022; Thiede et al., 2018; Xu et al., 2019)</p>	<p>Leverage collected business data to drive insights through big data analysis and support the decision-making process through AI:</p> <ul style="list-style-type: none"> <li>- Embed data-driven culture to adapt and provide insights into changing risk environment</li> <li>- Utilize data analytics to detect trends in changing risk early</li> </ul>
<p>Achieve strong IT and business alignment (Erol et al., 2010; Gomes, 2015)</p>	<p>Through enterprise architecture, firms have better insights into their implementation of information technology concerning their business goals, which makes it more achievable through increased visibility to improve Enterprise Resilience.</p>
<p>Digital operational resilience testing (Regulation (EU) 2022/2554, 2022)</p>	<p>The regulation on digital operational resilience for the financial sector that will apply in 2025, states an integral part of an IT Risk Management framework is a digital operational resilience testing programme (Article 24). Testing can occur in the form of vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, compatibility testing, performance testing, end-to-end testing, and penetration testing. High availability of digital services can be expected when extensive testing is done regarding digital operational resilience.</p>

## 4.2.2 Design choices and method dimensions

The design of the artefact has materialized in the form of a method. A method can be defined as a systematic and specific way of accomplishing something via a series of steps. Methods recommend and describe the procedures and techniques in detail that should be carried out.

Since the artefact is required to be practically implementable and must describe how the relevant stakeholders must behave, a method is the most suitable type of artefact. The resulting method presents detailed instructions at the strategic level that can lead firms to increased ER. The method is visualized to present the aspects of Information Systems Management and Risk Management and how they can be aligned. In order to visualize the method, the ArchiMate modelling language is utilized (The Open Group, 2023). Which is elaborated on in the following section 4.2.3.

The visualization of the method is divided into different dimensions. The definition of ER presented in section 3.2.1.3 makes a distinction between proactive and reactive measures to disruptions. Therefore, it follows that aspects that lead to ER must also be divided as proactive and reactive to visualize them in a logical sequence. Besides making a separation between aspects before a disruption and after a disruption, the state that a firm finds itself in during a disruption must not be forgotten. This state within a disruption is referred to in the model as the 'intra' disruption state. The distinction between proactive, intra, and reactive aspects is presented along the horizontal axis.

Some aspects that contribute to ER cannot be mapped in a causal sense, so they cannot be placed in the proactive, intra, or reactive category. These aspects describe in a more general sense how the organization must be governed. They are presented in a separate dimension under the name 'general governance'.

Along the vertical axis, a distinction is made between aspects of Information Systems Management and Risk Management. Furthermore, a third column is included that presents the overarching, causal process in which the aspects are aligned. This structure allows the aspects to be presented in their respective column in detail, the alignment between these aspects can then be presented in the third column which also connects the aligned aspects to form a course of action.

### 4.2.3 ArchiMate

The method is represented visually using the ArchiMate modelling language developed by The Open Group. ArchiMate is an open and independent enterprise architecture modelling language. Its general purpose is to support the description, analysis, and visualization of architecture within and across business domains in an unambiguous way (The Open Group, 2023). Typically, an enterprise architecture is developed because key people have concerns that need to be addressed by the business and IT systems within an organization. Therefore, it is suitable for visualizing different architectural domains and the underlying relations and dependencies.

Designing the method in the context of this research does not involve actual enterprise architecture, however, the structural objects and dimensions that ArchiMate offers make it a suitable language for the visualization of the method. The implementation of ArchiMate can generally be divided into three layers: the business layer, the application layer, and the technology layer. These layers align with the required structural elements needed for the design of the method. The layers can be identified by the colours as shown in Figure 12.

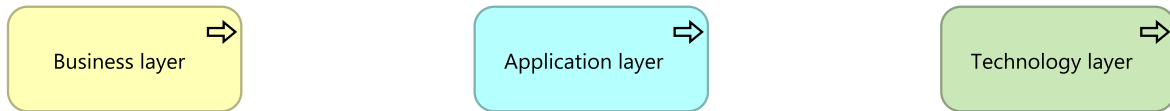


Figure 12: Business layer, application layer, and technology layer of ArchiMate (The Open Group, 2023)

The business layer is used to model the operational organization of an enterprise, the application layer shows the application architecture and how applications are used and interacted with, furthermore, the technology layer describes the technology infrastructure on which the applications are built. The technology layer can contain the software as well as the hardware infrastructure and the relations between them. Since the to-be-designed method attempts to match aspects from Risk Management and Information Systems Management the division of these layers is ideal for the development of a model that involves business aspects, but also the interaction with the IT estate.

Below, some additional ArchiMate structural elements are explained that are used in the visualization of the method.

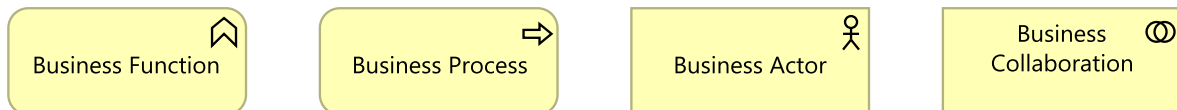


Figure 13: ArchiMate business layer elements (The Open Group, 2023)

Figure 13 shows the primary elements used in the method from the business layer. The *business function* represents a collection of business behaviours based on certain criteria such as business resources and/or competencies and is therefore often managed as a whole. Next, the *business process* represents one or a sequence of business behaviours that realize a product or service. A *business actor* represents a business entity that is in itself capable of performing behaviour, this can be a single actor, a group, or even a department. A *business collaboration* represents an aggregate of two or more business internal active structure elements that work together to perform some collective behaviour. It is used to represent a collaborative effort between two business actors.

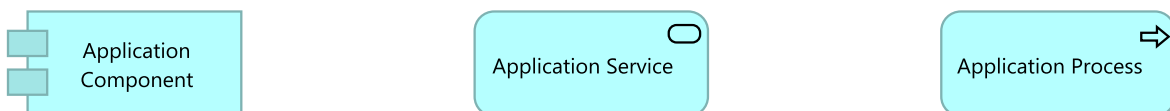


Figure 14: ArchiMate application layer elements (The Open Group, 2023)

The primary application elements used in the visualization of the method are shown in Figure 14. Firstly, the *application component* represents an encapsulation of application functionality. It can be used to model entire applications, but also parts of such applications, at all relevant levels of detail. An *application service* represents an explicitly defined exposed application behaviour, thus, an application service represents a distinct behaviour resulting from some application. And finally, the *application process* represents a sequence of behaviours that achieve a specific result.



Figure 15: ArchiMate technology layer elements, and value stream element (The Open Group, 2023)

Figure 15 shows the elements used from the technology layer. *Equipment* represents physical machines, tools, or instruments. A *facility* represents a physical structure or environment. Furthermore, Figure 15 shows a *value stream* element from the ArchiMate strategy layer. The strategy layer is an additional layer of ArchiMate used to model the strategic direction and choices of an enterprise. This layer contains the *value stream* element, which represents a sequence of activities that create an overall result for a customer, stakeholder, or end user. For the design of the method, the *value stream* is used to visualize the aligned aspects between ISM and RM. The aligned aspects describe on a strategic level the directions that must be followed.

Furthermore, ArchiMate contains a set of relationships that visualize different relationships between elements from all layers. The relationships used in the visualization of the method are shown in Figure 16. On the left, the *realization relationship* can be seen. It represents that an element plays a critical role in the creation, achievement, sustenance, or operation of another element. In the middle, the *triggering relationship* represents a temporal or causal relationship between elements. On the right, the *composition relationship* is shown, it represents that an element consists of one or more other concepts.

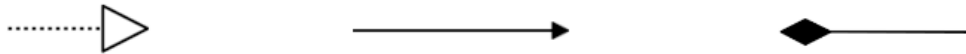


Figure 16: ArchiMate relationships: realization relationship, triggering relationship, composition relationship (The Open Group, 2023)

## 4.3 Validation approach

The treatment validation phase is executed using two instruments. Experts are interviewed and their insights into the relationships between Risk Management, Information Systems Management, and ER are gathered, also they are asked to reflect on the method. Furthermore, to test the applicability in a scenario that is close to actual implementation, a case study is performed. Cases concerning disruption were conceptualized, to which the method was applied in hindsight to observe the impact on the outcome of the scenario. Validation through interviews with experts is used in the first and second cycles, in the third and final cycle, the case studies are performed to get insights on the effectiveness of the finished product.

### 4.3.1 Gathering expert opinion through semi-structured interviews

The semi-structured interviews conducted during cycles 1 and 2 encompassed two distinct stages. The initial stage aimed to gather novel insights from experts by posing questions regarding the relationships in practice between Risk Management, Information Systems Management, and ER (refer to Appendix B for the full list of questions). This allows the experts to share their unbiased insights without first analysing the method.



The subsequent stage focused on the presentation of the method to the interviewees, allowing them time to analyse it and provide feedback. The discussion surrounding the method was an open conversation that was not constrained by preconceived questions, although the researcher guided the discussion by suggesting key points. These points of discussion corresponded to the fundamental dimensions upon which the method is built and the specific activities outlined within the method.

Each interview is fully transcribed and the main findings for each round of interviews are collected according to the methodology of semi-structured interviews described in section 2.2.2. The main findings of the interviews are presented in Chapter 5.

### 4.3.2 Apply the method in a case study

The optimal means of validation is through implementation. However, since implementation is outside the scope of the research, the most effective form of validation entails simulating the implementation process. To accomplish this, a qualitative case study is conducted, aiming to replicate the application of the method in a real-life setting, as outlined in section 2.2.3. Together with a candidate willing to participate, the method is applied retrospectively. Assessing the method's effectiveness within an actual setting holds the utmost value when the method's development has reached its peak maturity. Thus, the case study will serve as a validation mechanism exclusively during the final iteration of the design cycle. It is important to note that not every case may be suitable for every company, as certain industries are impacted to varying degrees by specific disruptions. Subsequently, the specific case is determined through collaborative discussions with the participant, aiming to identify a case concerning a disruption that has personally affected them and on which they possess substantial knowledge.

The case studies are divided into three primary components. Initially, the participant is interviewed to determine the level of ER prior to the disruption to establish a baseline. This is followed by the application of the method as if it were before, during, and after the disruption under the guidance of the researcher. Next, the method's usage is evaluated through a set of interview questions aimed at gathering perspectives and how the method would have impacted the company's resilience over the course of the disruption. Additionally, insights are gathered on the usage of the method itself in terms of usability and clarity. A detailed case description of an example case is given in Appendix C, which describes the objective, methodology, and expected outcomes of the case study. Although an example case has been defined, it is preferable to determine a case in collaboration with the participant.

As detailed in Appendix C, the initial phase of the case study involves establishing a baseline for the level of ER prior to the occurrence of the disruption. Although the method developed for this research incorporates a maturity tracker, which allows for insights into the maturity of ER, an alternative methodology is employed to establish the initial baseline. To this end, a brief questionnaire defined by Hollnagel (2010) is utilized, aimed at determining the level of ER of a firm. The questionnaire is founded on four fundamental abilities of resilience as outlined by Hollnagel (2010), namely, monitoring, anticipating, responding, and learning. These abilities are further elaborated upon in a subsequent chapter dedicated to the design of the method. By utilizing a set of questions, each of these abilities is rated on a scale ranging from 'missing' to 'excellent'. Employing an alternative and established methodology for assessing ER maturity ensures the avoidance of introducing bias. If the measurement instrument used to gauge the



level of ER is based on the method being tested, it can lead to significant biases that hinder accurate measurements.

Once the baseline for ER has been established, the simulation of applying the method commences. Under the guidance of the researcher, the participant is instructed to apply the method as if they were facing the described disruption in the case study. The participant will carefully analyse each activity within the method and assign a maturity level to it. While the researcher is available to answer any questions, the aim is to allow the participant to independently apply the method. The researcher's clarifications are only provided to ensure adherence to the allotted time frame and to remain in control of any unknown variables that might emerge.

The subsequent step in the application of the method involves identifying activities that require improvement based on the assigned maturity levels. The participant is asked to justify their decisions regarding which activities warrant resource allocation, as well as why certain activities may not receive resource allocation. This examination provides insights into the effectiveness and feasibility of the specified activities within the method.

Following this, the questionnaire used to determine the level of ER (Hollnagel, 2010), which was employed to establish the baseline, is revisited with the participant, taking into account the discussed activity improvements. Comparing these results with the baseline outcomes provides insights into the effects on the level of ER. Building upon these findings, the anticipated outcome of applying the method in the context of the disruption is examined and discussed. Additionally, the participant is asked further questions regarding the potential effects of the method according to their beliefs.

Upon completion of the simulation, the participant is prompted to reflect on the method's usability, clarity, and feasibility. The comprehensive set of questions utilized during the case study can be found in Appendix D.

By comparing the resulting level of ER with the baseline, a general conclusion can be drawn regarding the effectiveness of the method. This is strengthened by the motivation of the participant regarding their experiences while applying the method. The audio of the complete case study process is recorded. The recordings are transcribed and analysed to gather insights.

## 4.4 Summary

Chapter 4 covers the requirements for the design of the method, as well as further methodological considerations related to the design choices and the used instruments. The chapter begins by introducing and motivating the requirements that the final method must adhere to in section 4.1. These requirements are considered valid only if they contribute to the goals of relevant stakeholders. Section 4.2 describes the guidelines for designing the method, including the description of the initial method and the design choices made for its structure. Additionally, section 4.3 introduces the instruments that are involved with the validation of the method.

The requirements are divided into functional and non-functional requirements. Functional requirements describe what an artefact must do, and what its functions and features are. Non-functional requirements are global properties of the interaction between the artefact and its

context. It describes how the system goes about delivering a specific function. Both types are specified to ensure a method that is both functional and practical.

The design approach of the method is based on data collected from literature and expert opinions obtained through semi-structured interviews. The initial version of the method is designed based on findings from literature and alternative treatments, and it serves as a basis for further iterations through the design cycle. The design choices that give structure to the method are also described. The method is designed using the ArchiMate modelling language, which is introduced. These aspects together form the initial version of the method.

Similarly, the validation instruments are introduced. Initially, the method is validated through interviews with experts. The final iteration involves a case study that aims at simulating the implementation of the method.

# 5 Development

This chapter aims to describe the sequence of activities undertaken during the development of the proposed method. These activities are presented in a sequential order that mirrors their actual execution. A comprehensive overview of the executed cycles can be found in section 2.1.3, while the specific activities pertaining to each cycle are provided in Table 15 below. The ensuing sections are dedicated to expounding upon the distinct phases of the treatment design and treatment validation phases. Each section is further divided into subsections, addressing the individual phases comprehensively. By adhering to this structured approach, a comprehensive understanding of the entire design process, as delineated by Wieringa (2014), can be achieved. At the culmination of cycle 2, the development process reaches a state wherein all pertinent information has been gathered, this chapter details the complete development process up until that point. Subsequently, the following Chapter 6 outlines the conclusive design considerations for the final iteration of the method, and this concluding iteration of the ER enhancement method is presented.

*Table 15: Design cycle activities*

<b>Cycle</b>	<b>Problem investigation</b>	<b>Treatment design</b>	<b>Treatment validation</b>
1	Stakeholder analysis Literature review	Design initial artefact using literature and available treatments	1 <sup>st</sup> round of interviews with experts
2	Re-evaluate stakeholder drivers and goals	Redesign based on cycle 1 validation	2 <sup>nd</sup> round of interviews with experts
3	Re-evaluate stakeholder drivers and goals	Redesign based on cycle 2 validation	Case study

## 5.1 Cycle 1

### 5.1.1 Design: The initial artefact

By combining all elements described in section 4.2 an initial version of the method was designed. ArchiMate (section 4.2.3) was used in a slightly alternative way as the modelling language for designing the method. The design choices described in section 4.2.2 define how the method was formed in terms of the dimensions. Furthermore, the identified aspects of available treatments described in section 4.2.1 were used to fill out the method with initial aspects leading to ER as described in the literature.

The culmination of these endeavours resulted in the generation of an initial method design, depicted in Figure 17 below, named the 'ER enhancement method'. It is important to note that this initial design is primarily based on insights derived from the literature, thus necessitating validation through engagement with practitioners. This validation process is imperative to gain a comprehensive understanding of the method's potential effectiveness in practical contexts.

As delineated in section 4.2.2 pertaining to the design choices and dimensions, the method comprises three primary columns. The leftmost column encompasses activities commonly associated with Risk Management, which have been substantiated through literature as contributors to the establishment of ER. Similarly, the right column contains activities pertaining to Information Systems Management that also contribute to the development of ER. The objective of the middle column is to effectively align these activities. To achieve this, the activities leading to enhanced ER, as outlined in Table 13 and Table 14, were considered for alignment with one another. By identifying activities that potentially reinforce one another, aligned activities were established in the middle column. Currently referred to as 'process,' this name is not exhaustive and will be revised in subsequent cycles.

The following requirements were set for the activities to be considered aligned:

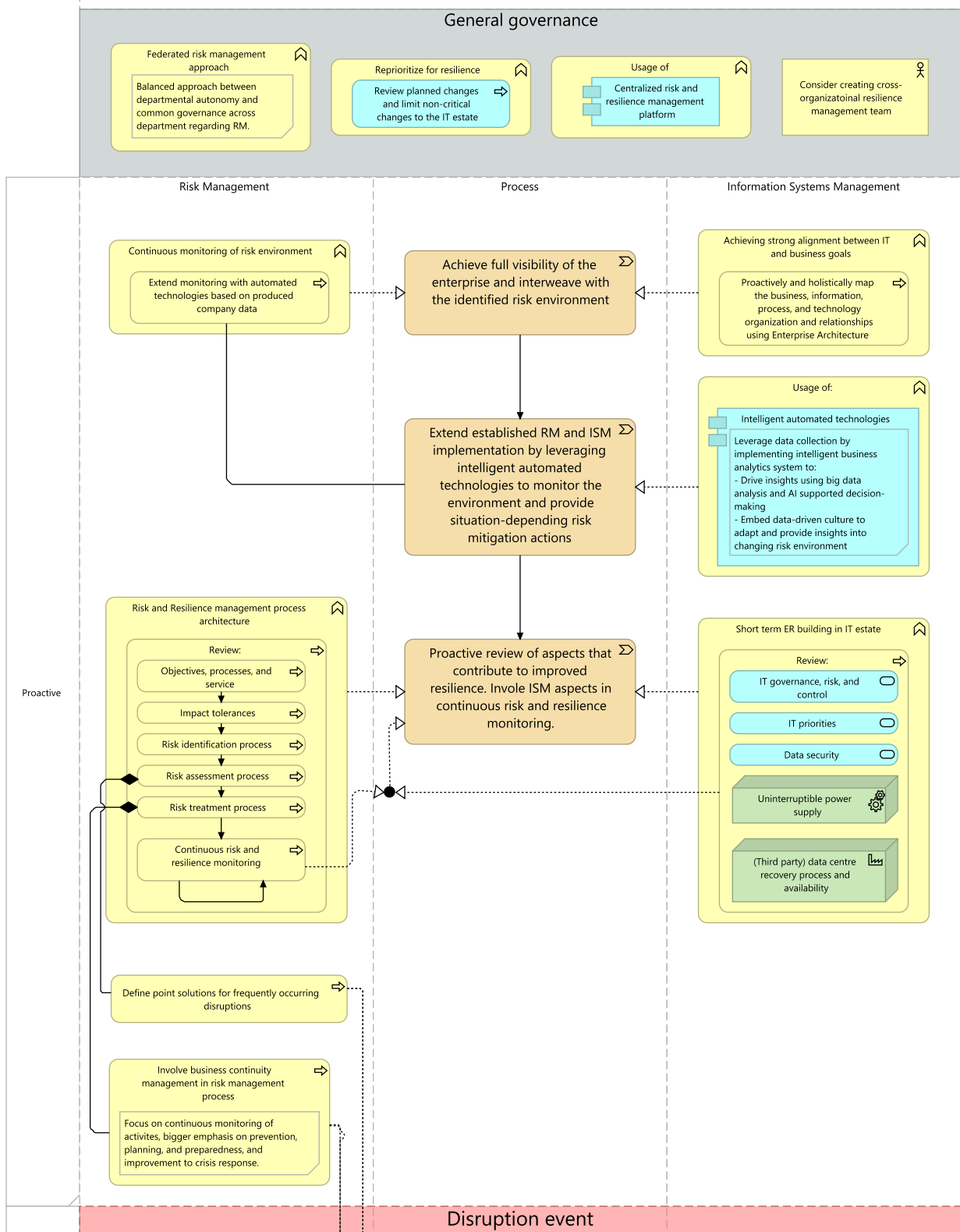
- The distinct activities must be interwoven with each other. The aligned activity describes a resulting company function, while the distinct activities specify how this function should be fulfilled or implemented.
- If there is any conflict between RM and ISM activities, the aligned activity must minimize the conflict to a negligible extent.
- If the RM and ISM activities are compatible and do not conflict, the aligned activity in the middle column should be an enhanced amalgamation of the two distinct activities.

After aligning the activities, an effort was made to arrange the Risk Management, Information Systems Management, and aligned activities in a coherent sequence within the method. In accordance with the discussion presented in section 4.2.2 concerning design choices and dimensions, it was deduced from the literature that the construction of ER entails the execution of proactive and reactive activities. Furthermore, insights from the literature indicated the inclusion of activities as an immediate response to the occurrence of a disruption. These activities were categorized as 'intra', denoting actions that must be undertaken promptly during a disruption. These three primary categories constitute the division of rows within the method. As illustrated in Figure 17, the proactive activities are depicted first, followed by the intra-activities marked in red, and finally, the reactive activities subsequent to the onset of a disruption. Subsequently, the aligned activities were allocated to their corresponding rows within the method. The placement of these activities was guided by the principle of maintaining a logical order based on causality. For instance, the initial activity involved acquiring comprehensive visibility of the enterprise and intertwining it with the identified risk environment. This step of fully mapping the enterprise and its associated risks serves as a foundation for subsequent activities.

Furthermore, a supplementary row titled 'general governance' is positioned at the top of the method. These activities were not aligned with any existing rows of the method, as they encompass general company functions that are essential for enhancing the overall effectiveness of the comprehensive method.

The resulting initial version of the method was subjected to validation in the subsequent validation phase described in the next section. The method is validated through opinions of the expert practitioners and the adherence to the pre-specified requirements is tested.

# Enterprise Resilience enhancement method



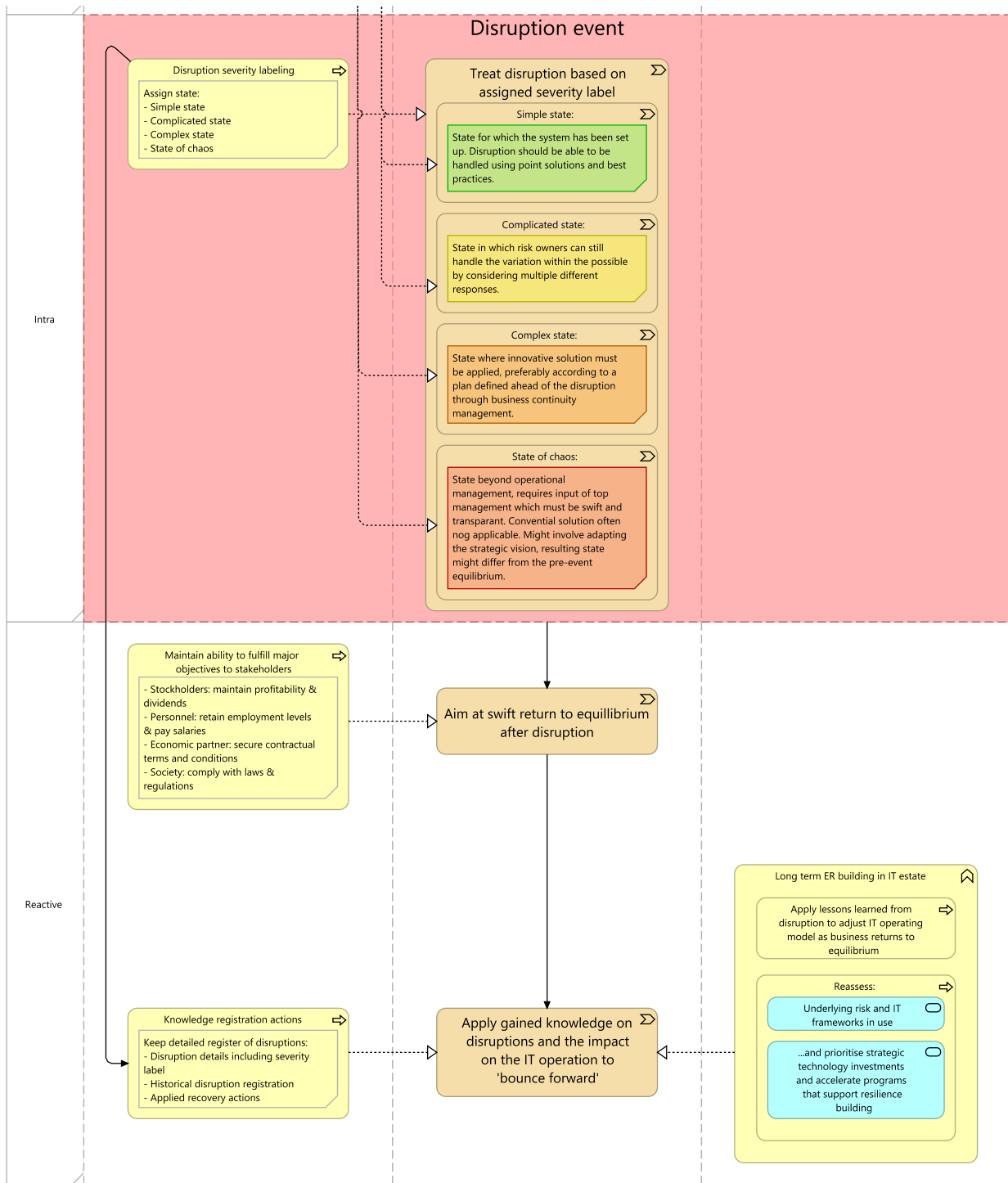


Figure 17: Initial design based on literature findings (ER enhancement method, cycle 1)

## 5.1.2 Validation: Interviews & Requirement satisfaction

Treatment validation in cycle 1 consists of two parts. First, the method is validated by discussing it with experts and collecting their feedback and insights on it. Second, it is verified whether the method complies with the requirements that were set and described in section 4.1.

### 5.1.2.1 Expert opinion through interviews

The first round of semi-structured interviews was partly used to validate the initial version of the method. The validation was conducted by introducing the method to the interviewee and providing them a moment to consider feedback. In addition, the interviewees were asked to provide new insights not yet present in the method. The approach is discussed in more detail in section 4.3.1.

All interviews were conducted according to the guidelines described in section 2.2.2. As mentioned in this section, purpose sampling was the method used to select candidates for interviews. Different profiles were created that define the characteristics that are desired for interview candidates. Table 16 shows the data that was collected on the participants of the interview, they can be identified by their interviewee ID, which from this point is used to refer to them. The interviewees were selected to fit the profiles described in Appendix A.

*Table 16: First-round interviewees' data*

<b>Int. ID</b>	<b>Job title</b>	<b>Years in current position</b>	<b>Company sector</b>	<b>Estimated no. of employees</b>
1.1	Expert Lead Data Risk, previously wrote company policy on operational resilience	5 years in current position, +/- 25 years in risk and IT	Wholesale & retail banking	50.000+
1.2	Senior Enterprise Risk Manager	10 years	Asset Management for Pension fund	Total 3.000+, +/- 200 at branch
1.3	Head of Resilience	11 years	Asset Management for Pension fund	Total 3.000+, +/- 200 at branch

The main point of feedback from interviewee 1.1 was on the addition of iteration to the method. Internally at the company of interviewee 1.1, ER building is considered a continuous process based on a cycle of four abilities. The cycle contains the ability to anticipate, the ability to monitor, the ability to respond, and the ability to learn. The cycle implies that when a firm has learned from disruption, a shift towards anticipating has to be made, which restarts the cycle. Baking in a continuous aspect into their strategy ensures resilience is a constant priority that remains important even when a disruption has passed.

The abilities mentioned by interviewee 1.1 can be mapped to the three main phases in the initial method seen in Figure 17. All proactive activities are concerned with anticipating disruptions by building measures and controls in the business processes and IT estate. Similarly, the ability to monitor can also be identified in the method, since monitoring the risk environment and many likely sources of disruption, is very apparent within the proactive

activities described in the initial method. Furthermore, how to respond to disruption is described in the intra-phase which takes place during a disruption. And lastly, the ability to learn is described in reactive activities. The focus on learning fits very well with the significance the initial method puts on 'bouncing forward'. Therefore, a similar cyclic approach is adopted in the next version of the artefact that promotes continuous resilience building.

A major point of feedback by interviewee 1.3 was regarding the absence of people described in the method. In their experience, people are one of the most important resources when facing disruption. It was discussed during the interview that possibly another vertical lane could be added that contained the most important people relevant to the described activities in the other lanes. Also, the relevance of a resiliency management team or position was discussed. This entity is mostly concerned with constant monitoring and consequently reporting constantly on disruptions. Additionally, it focuses on building towards a company-wide culture that is focused on operating in a resilient manner. Also, a crisis management team is a valuable resource when the right people are on it. It must contain decision-makers (CEO, CFO, head of facilities), business representatives of all parts of the business (head of HR, legal representative, etc.), but also information providers that are fully aware of the situation (resiliency management team/person). The importance of people as a resource is a valuable addition to the model because, in a practical sense, it increases the adoptability of the method since responsibilities are described. The inclusion of people was also mentioned by interviewee 1.2 as an important resource.

Additionally, several activities in the initial method were discussed separately with the interviewees. Based on the validity of the discussion certain activities and aspects were altered according to the feedback. The activity of reviewing 'data security' was extended, to reviewing the data resilience. On top of security, data resilience also involves ensuring data quality, redundancy, and availability. Furthermore, the main priority of the cross-organizational resilience management team was discussed. Among other responsibilities, the interviewees mentioned the team's focus should be on installing a resilience-focused culture across the organization. It was also mentioned that the threshold for the different disruption severity states were missing which might make it difficult for a firm to assign a state to a disruption. Although exact states cannot be defined since this is dependent on company size and sector, the possible metrics that can serve as thresholds can be introduced in the method.

In addition, all interviews were asked to answer the same set of questions during the semi-structured interview to gather new insights not yet present in the method. The questions are presented in Appendix B. From there, the researcher allowed the interview to take on a free-flowing conversation style as is usual with semi-structured interviews. This resulted in the findings presented in Table 17.

*Table 17: Main findings from the first round of interviews*

<i>Int. ID</i>	<b>Findings</b>
1.1	The abilities to; <b>anticipate, monitor, learn, and respond</b> help enterprises in behaving in a manner that is resilient. They are the four essential abilities needed for achieving ER. These four essential abilities are fundamental for achieving ER. However, it is imperative to emphasize that continuous and iterative practice of these abilities is essential to attain optimal results. The ability to anticipate can be



implemented by applying resilience-by-design. The ability to monitor can be implemented by (real-time) monitoring and alerting, and defining the threshold vs the targets. The ability to learn can be implemented by root cause analysis or having an open culture to learning from failure.

- 1.1 An important difference relating to **operational resilience** that the firm of interviewee 1 has made is to consider it from the perspective of the consumer when it comes to their services. They measure operational resilience in terms of the **consumability** of the customer or regulator that needs to access their systems. Internal disruptions are registered but they do not impact the consumability of the services. Targets are set for the consumability of services, the responsible entity has autonomy on how these targets are accomplished. For digital services, targets and thresholds are also described by COBIT control and ITIL processes.
- 1.1 **All Risk Management activities** contribute to Enterprise Resilience, the focus should be on executing these activities in a resilient way.
- 1.1 An **additional state** for disruption can be expressed in terms of **consumability**. The most severe state would have an impact on the consumability of the services. A state below this in terms of severity might not impact the consumability, but internal processes or functions are disrupted. However, this is considered less severe by the company of interviewee 1 because consumability is not affected.
- 1.1 **Dynamic Risk Management** can be a powerful tool towards building Enterprise Resilience. It involves being prepared for the unknown by being aware of what is happening in the world around you.
- 1.1 In order to measure the level of operational resilience, **targets** and **thresholds** can be set as the limit for each state. Target and thresholds can be set on the consumability of digital services, but also on other aspects that relate to operational resilience like equipment downtime,
- 1.2 The usage of internal **governance and risk tooling** supports holistic Risk Management by having process owners report on the issues or controls from a risk framework. This is then reviewed by risk managers and recommendations or provided to optimize the mitigation of risks. 'B Wise' is used by the company of interviewee 1.2 for this purpose. ('B Wise' was recently acquired by SAI360<sup>1</sup>)
- 1.2 Having **great knowledge of all processes** is crucial to **identifying risks**. This allows you to find a way to mitigate most risks, besides this, measures based on best practices must be in place for residual risks that cannot be identified proactively.
- 1.2 Thresholds are used to label disruption in terms of severity. A measure that is used is the **financial impact**. If the financial impact is expected to be larger than a certain threshold the board must be informed, even if no solution is available yet. This is then followed by a **root cause analysis**, which is used to discover the root of problems in order to identify appropriate solutions.
- 1.3 **Change management** must be performed in a **resilient matter**. The process of adopting change should be executed with Enterprise Resilience in mind, examples

<sup>1</sup> <https://www.sai360.com/about-us/bwise-is-now-sai360-grc>

	are: Considering recovery when adopting a new application, implementing redundancy, or doing an impact analysis on related systems.
1.3	Perform regular <b>exercising</b> and <b>testing</b> , while making sure the people who are actually going to be challenged during the incident partake in the exercise to build <b>muscle memory</b> . Crisis response plans, point solutions, business continuity plans, disaster recovery plans, and digital operational resilience plans must all be tested.
1.3	Resiliency manager/team is responsible for providing as much <b>information</b> as possible to senior management during a disruption, so they can make a logical decision. The resiliency manager/team must provide unbiased information from unbiased sources. Also, a <b>communication plan</b> must be defined to keep the entire company informed with unbiased information as soon as a disruption occurs.
1.3	In terms of cyber resilience, make sure where the <b>crown jewels</b> of your organization are. Although you want to protect everything, priority must be given to the crown jewels. Crown jewels are the data without which your business would have difficulty operating, or data that is a high-value target for cybercriminals.
1.3	Consider the usage of an <b>enterprise-wide, multimodal communication tool</b> that informs all relevant stakeholders instantly through multiple platforms on a disruption and its severity. (Example: Send Word Now)
1.3	Incident severity is measured first in terms of <b>impact on employees (safety)</b> , and secondly in terms of impact on the business. The impact on the business could be measured by whether critical functions are still in place.
1.3	Your crisis plan needs to be nimble enough to adjust to most of the common risks out there; man-made disasters, natural disasters, and cybersecurity disasters. However, you cannot have a playbook for everything, in these situations: <b>gather all information before making snap decisions</b> .
1.3	Subscribe to <b>continual streams of possible sources of information</b> : local, regional, and national emergency services updates, governmental updates, unbiased news updates, traffic & public transport updates, extreme weather & natural disaster updates, and any other information streams relevant to your business.

### 5.1.2.2 Requirement satisfaction

The second part of validation in the first cycle is verifying to what extent requirements are satisfied by the current design of the artefact pictured in Figure 17. The functional- and non-functional requirements the method must adhere to are specified in section 4.1. This section reflects on these requirements and lists possible improvements. The requirements that have not been complied with in the initial method are listed and examined in the remainder of this section.

The requirements F2, F3, F4, and F5 are concerned with how both the Risk Management department and IT department must behave strategically, and how their processes must be structured. Additionally, the cooperation between the departments must be described according to F6. Although major strategic actions are described for both departments in the initial method in Figure 17, responsibilities for specific stakeholders are not described. Thus, to implement these requirements to a fuller extent people may be included in a consequent

version of the method. The same conclusion followed from the expert opinions (section 5.1.2.1), therefore, one of the main goals for the next iteration of the method is to include people and assign them to activities where possible.

NF1 describes the requirement for scalability with the risk environment a firm finds itself in. The initial method does not describe any distinction between how to apply it to companies in a low or high-risk environment. The next iteration must therefore specify how to adopt the method in different risk environments.

According to NF2, the method must be practically implementable and usable. And although the activities are all practically implementable, the method as a whole was described during the interviews as 'difficult to read' due to its size and might therefore be abandoned. During the next design phase, an attempt is made to make the method more tangible, either through redesign of the dimensions or an alternative support tool.

Requirement NF4 is concerned with continuous ER improvement, which is missing in the initial artefact. The continuous nature of resilience was also mentioned in the interviews with experts, with the suggestion to make build the method around a cyclic process.

## 5.2 Cycle 2

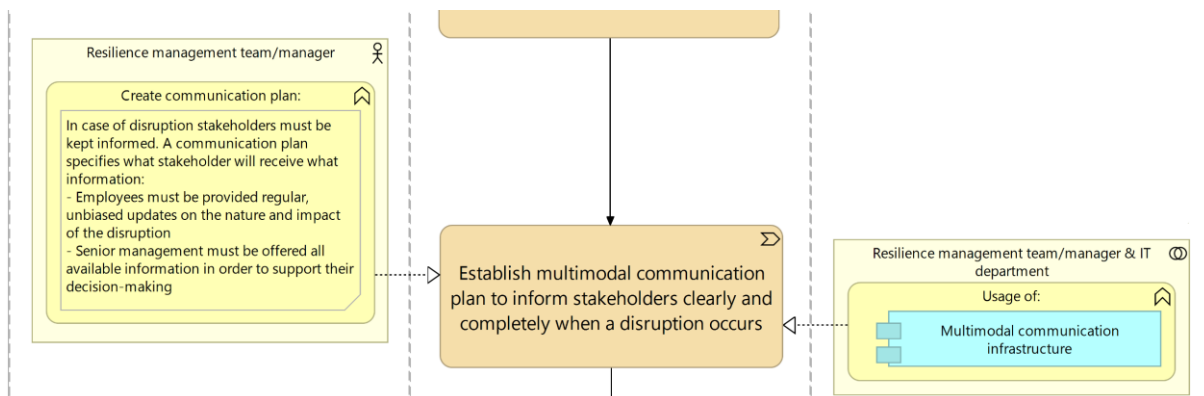
### 5.2.1 Design

The initial round of interviews was primarily focused on knowledge acquisition from experts in relevant fields pertaining to the research topic. The individuals listed in Table 16 were interviewed not only to validate the proposed method but also to gain their perspectives on the research topic prior to being exposed to the method itself. This approach ensured that the interviewees could express their opinions on the interconnections between Information Systems Management, Risk Management, and ER without any external influences. During the interviews, all participants were presented with identical sets of queries, which can be found in Appendix B. From there, the researcher allowed the interview to take on a free-flowing conversation style as is usual with semi-structured interviews. This resulted in the findings presented in Table 17.

The findings obtained from the first cycle's validation process were analysed and employed to develop an updated version of the method. This intermediate iteration of the method is depicted in **Appendix E**. The findings from the interviews found in Table 17 resulted mainly in additional activities on both the Risk Management and the Information Systems Management side of the method. They have been fully integrated with the aligned ER-building process in the middle column, which was renamed accordingly. Although efforts were made to arrange these aligned activities in a logically causal manner, it is crucial to note that this aspect still requires validation by subject matter experts. Furthermore, the two key findings from the validation process involving experts during the initial cycle (section 5.1.2.1) have also been incorporated into the updated method. These findings involve the addition of people and the restructuring of the method to follow an iterative approach, thereby establishing it as a continuous process.

The incorporation of people within the method was accomplished by assigning a responsible actor to each activity. This representation of people was achieved by placing all activities within an additional box that signifies the involvement of people. Furthermore, the presence of the business collaboration object (as specified in section 4.2.3 of the ArchiMate specification) can be observed surrounding certain activities, indicating a collaborative effort between two or more responsible parties. The aligned activities situated in the middle column naturally are assigned to the individuals accountable for the Risk Management and Information Systems

Management activities depicted in the side columns. By incorporating people within the method, the implementation process becomes more accessible, as the assignment of specified activities becomes more tangible and actionable. An example of the introduction of people into the method is depicted in Figure 18. The activity to create a communication plan is assigned to the resilience management team/manager. Additionally, when an activity is assigned to multiple people, the collaboration element of ArchiMate is used. An example of this is also shown in Figure 18, the resilience management team/manager and the IT department must collaborate on the implementation of a multimodal communication infrastructure.



**Figure 18: Addition of people and collaborations to the ER enhancement method**

During the cycle 1 validation, interviewee 1.1 provided valuable insights regarding their internally developed model for building and maintaining resilience. This model was built upon the existing research by Hollnagel (2013), who initially outlined the four essential abilities of resilience: monitor, anticipate, respond, and learn.

The ability to anticipate is concerned with knowing what to expect or being able to anticipate developments further into the future, such as potential disruptions. The ability to monitor revolves around knowing what to look for or being able to monitor that which is or could seriously affect a firm's performance in the near future. This includes the firm's own performance as well as what happens in its environment. Then there is the ability to respond, knowing what to do, or being able to respond to regular and irregular changes and disturbances, but also opportunities by activating prepared actions. And finally, the ability to learn is concerned with knowing what has happened or being able to learn from experience, in particular, to learn the right lessons from the right experience.

These abilities align closely with the dimensions incorporated within the ER enhancement method. The proactive abilities of anticipation and monitoring contribute to enhancing preparedness before a potential disruption occurs. The ability to respond becomes crucial once a disruption takes place and is essential during its occurrence. The 'intra' dimension is similarly designed to capture critical activities during the presence of a disruption. Finally, the ability to learn aligns precisely with the reactive abilities, emphasizing the importance of effectively learning from disruptions and leveraging that knowledge to 'bounce forward'.

Following these observations, the rows representing the different phases of a disruption were further labelled to reflect the corresponding critical abilities during each phase: proactive (abilities to anticipate and monitor), intra (ability to respond), and reactive (ability to learn).

As elucidated in the findings derived from the validation process (section 5.1.2.1), the building of ER is an ongoing and iterative endeavour. It is crucial to perceive the development of ER as a continuous, cyclic process. As previously mentioned, interviewee 1.1 devised a foundational model for building resilience based on the research by Hollnagel (2013). A significant

enhancement introduced in this adapted version was the incorporation of a cyclic aspect to the four essential resilience abilities. A specific sequential order was established: anticipation, followed by monitoring, response, learning, and then returning to anticipation. This iterative approach fosters a resilient mindset that extends beyond mere survival, emphasizing growth and advancement. This model has since been adopted by the company of interviewee 1.1.

Given that the four abilities have been aligned with the ER enhancement method, the cyclic nature can be similarly embraced. This is implemented by integrating a pivotal activity within the aligned pathway of activities in the middle column. Once the learning activities have been executed or are underway, the focus must gradually transition back to anticipation and monitoring. This ensures that the lessons learned are promptly applied in preparation for the inevitable occurrence of future disruptions.

All aforementioned modifications were successfully integrated with the initial method resulting in the updated ER enhancement method depicted in Appendix E. The subsequent phase entails once again conducting a validation process, as mentioned in Table 15, this consists once more of semi-structured interviews to gather new insights and observations on the method.

## 5.2.2 Validation: Interviews & Requirement satisfaction

In cycle 2, treatment validation again comprises two distinct components. Firstly, the method undergoes validation through expert opinion using interviews. Secondly, a verification process is conducted to assess whether the method aligns with the pre-established requirements outlined in section 4.1.

### 5.2.2.1 Expert opinion through interviews

Validation during cycle 2 is similar to cycle 1 (section 5.1.2), once more semi-structured interviews are executed to gather new insights and feedback from expert practitioners. A new set of interviewees was recruited for validation in cycle 2. The interviewees were once again chosen to fit closely to the profiles described in Appendix A shows the chosen experts for cycle 2 validation.

*Table 18: Second round interviewees' data*

<b>Int. ID</b>	<b>Job title</b>	<b>Years in current position</b>	<b>Company sector</b>	<b>Estimated no. of employees</b>
2.1	IT Audit & Risk Officer (Partner at firm)	5 years	Auditing & Consultancy	8
2.2	IT Risk Manager	4 years	Insurance & asset management	15.000+

Once again, the questions described in Appendix B formed the basis for the interview. From there, the researcher allowed the interview to take on a more free form of conversation. The main findings from the interviews are shown in Table 19.

*Table 19: Main findings from the second round of interviews*

<b>Int. ID</b>	<b>Findings</b>
----------------	-----------------

- 2.1 The role of **culture** in fostering enhanced Enterprise Resilience is of paramount importance. Bureaucratic organizations often encounter challenges due to their relatively rigid cultural norms that exhibit resistance to evolution and growth. Conversely, startups serve as exemplars of flexible organizational structures that possess the ability to adapt to dynamic environments. Thus, cultivating a culture characterized by a proactive willingness to embrace change emerges as a critical prerequisite for the cultivation and advancement of Enterprise Resilience.
- 2.1 The second line of defence, as established in the 3 lines of defence (3LOD) model, is responsible for enabling the identification of emerging risks, it does this by compliance and oversight in the form of framework, policies, tools, and techniques to support risk and compliance management (The Institute of Internal Auditors, 2020). In terms of Enterprise Resilience, **establishing an excellent second line of defence is crucial**, e.g. an excellent CISO. Excellence refers in this case to a capable, convincing person that can install a positive culture towards mitigating risk and building resilience.
- 2.1 In today's business landscape, companies of various scales enjoy convenient access to third-party IT infrastructure providers such as AWS, among others. Nonetheless, despite the accessibility of these resources, the **escalating aggressiveness of risk environments**, driven by emerging threats like ransomware, implies that the mere availability of third-party IT infrastructure **does not automatically guarantee heightened levels of digital operational resilience**.
- 2.2 A dedicated **business continuity management officer** takes care of organizing the business continuity plans. An effective way of organizing this is using a **bottom-up approach**. Which involves lower-level employees working towards a certain goal. This ties into a crucial finding of this research, which is to importance of installing a resilient-aware culture with all employees.
- 2.2 The implementation of an **internal alert system** designed to monitor potential disruptions provides an organization with the ability to proactively identify and anticipate impending IT disturbances. This objective can be achieved through the deployment of early monitoring tools, which aim to enhance the company's resilience. In the case of interviewee 2.2's organization, the implementation of Splunk<sup>2</sup> tooling serves this purpose. This tooling enables the establishment of thresholds for various IT elements, such as database utilization. By incorporating this tooling into its operations, the organization endeavours to maximize the recognition of early warning indicators.
- 2.2 Caution must be exercised when undertaking efforts to enhance a comprehensive concept like Enterprise Resilience. In the case of Interviewee 2.2's company, it was explicitly stated that a deliberate improvement program targeting cyber resilience is in place. This deliberate approach aims to **counteract the potential misconception among individuals that they are not directly implicated by such initiatives**. Hence, when considering the methodology's design, it is imperative to ensure that the majority of individuals perceive their involvement in the implementation process as significant.

<sup>2</sup> [https://www.splunk.com/en\\_us/home-page.html](https://www.splunk.com/en_us/home-page.html)



- 2.2 Testing is a crucial part of building resilience, as already specified in the method. However, on top of the **'table top' exercises**, during which a crisis is simulated, **'real' tests are offered in which a third party attempts to create a real IT crisis in a controlled way**. This way the measures are truly tested by recreating a sincere crisis.

The findings presented in Table 19 were carefully examined in relation to prior research findings and deemed to be valid. In addition to uncovering novel insights, a comprehensive validation of the existing method was undertaken through collaboration with the interviewees. This collaborative process led to a series of adjustments, ranging from minor to moderate, which were discussed in order to ensure their validity. These modifications encompassed various aspects, such as enhancing clarity through minor revisions and rectifying inaccuracies by rewriting descriptions that were found to be imprecise.

Furthermore, by conducting a thorough analysis of comparable content pertaining to the proposed design, the notion emerged to augment the existing method with a maturity model. Within the realm of consultancy, it is customary to evaluate the maturity of specific aspects of firms using maturity models. Consequently, in consultation with an IT assurance senior consultant from a consulting firm, an expansion to the established method was conceptualized in the form of a maturity tracker, which is used to measure the maturity of a particular process, capability, or organizational area, providing a roadmap for improvement. For the purpose of illustration, Appendix F depicts a maturity matrix used to measure the continuous monitoring and continuous auditing of a consulting firm. A similar approach is used to design a maturity tracker related to the method, with the goal of extending the method's functionality. This proposition was proposed and deliberated upon during the cycle 2 interviews with subject matter experts. The consensus reached was that the inclusion of a maturity tracker enhances the method's tangibility, as it empowers users to position themselves on a scale for each of the aligned activities. The primary objective behind the development of the maturity tracker is to enable users to assign maturity levels to these activities, thereby gaining valuable insights into potential areas for improvement in pursuit of achieving ER and making the adoption of the method more tangible.

### 5.2.2.2 Requirement satisfaction

Once again, an analysis is made as to whether the current version of the method depicted in Appendix E adheres to the pre-specified requirements (section 4.1). The initial design resulting from cycle 1 (Figure 17) already met a part of the requirements, as described in section 5.1.2.2. The requirements that were not yet satisfied are addressed again in this section.

The requirements F2, F3, F4, and F5 pertain to the strategic behaviour and process structure of both the Risk Management department and the IT department. Additionally, F6 addresses the need to describe the collaboration between these departments. In the initial assessment of requirements satisfaction during cycle 1 (section 5.1.2.2), it was determined that while the behaviours were described, they were not specifically assigned to people. Consequently, no complete definition of the strategic behaviours expected from the departments was given. To address this, the updated method incorporates the inclusion of people to a greater extent, aligning with the requirements F2, F3, F4, F5, and F6, as detailed in section 5.2.1. However, additional improvement may be possible still. As discussed in the preceding section, the method could benefit from the integration of a maturity tracker. Such a tracker would provide

clarity on the expected behaviours by defining maturity levels to strive for within the departments.

NF1, which pertains to the scalability of the method to accommodate diverse risk environments of different companies, was previously assessed as not being fully met. During the design phase of cycle 2, certain modifications were introduced to adapt the activities to suit a wider range of risk environments. However, a delicate balance must be struck between ensuring accessibility for companies in various risk environments without compromising specificity. Thus, the fulfilment of this requirement may necessitate additional attention during the design phase of cycle 3.

However, the inclusion of the maturity tracker provides descriptions for different levels. Consequently, companies operating within less aggressive risk environments can focus on achieving maturity level 3. This level aims to generate a positive impact on ER without requiring a substantial allocation of resources, which aligns with a less aggressive risk environment.

The subsequent aspect to be addressed is NF2, which pertains to the practical applicability and usability of the method. The adoption of a maturity tracker enhances the method's accessibility and tangibility. This contributes to the usability of the method, as acknowledged by the participants during the validation phase of cycle 2.

During the design phase of cycle 2, the method was altered to become continuous. Meaning at the end of the reactive activities, the suggestion is made to return to the proactive activities to once more review and improve the ability to monitor and the ability to anticipate. By incorporating this continuous feedback loop, the requirement NF4, which pertains to the continuous aspect of improving ER, is fulfilled.

The implemented modifications have resulted in the fulfilment of all requirements to an improved extent, if not entirely. As a result, the forthcoming design phase of cycle 3 focuses on making minor adjustments to ensure full compliance with all pre-defined requirements. The conclusion of cycle 3 involves an analysis to determine the extent of adherence to all requirements. Therefore, section 5.3.2.2, which addresses requirement satisfaction after cycle 3, provides a comprehensive list of all requirements and offers justifications for the manner in which they were implemented.

All discussed content is expounded upon in the consequent chapter. The final design considerations based on the findings of the treatment validation phase of this cycle are processed and the resulting concluding iteration of the ER enhancement method is presented.

## 5.3 Summary

Chapter 5 elucidated the development of the ER enhancement method, which encompassed both design and validation phases in accordance with the Design Science Methodology proposed by Wieringa (2014). Recognizing the iterative nature of the design cycle, the process was divided into discrete cycles. The primary development phases were carried out in the initial two cycles, as depicted in Table 15, while the concluding cycle focused on the final redesign, and validation through a comprehensive case study, which is expounded upon in the subsequent chapter.

The design phase of cycle 1 primarily entailed the translation of theoretical findings from the literature into an initial iteration of the ER enhancement method. Subsequently, expert opinions



were sought to validate this initial iteration through the employment of semi-structured interviews.

Building upon the insights garnered from the preceding validation process, the design phase of cycle 2 involved synthesizing the information acquired from the interviews to create an updated iteration of the ER enhancement method. Once again, semi-structured interviews were conducted to validate the modifications and additions. At this stage, all pertinent information was gathered to finalize the iterations and arrive at a conclusive version of the method, which is presented in Chapter 6.

---

# 6 ER Enhancement Method

---

The design and development efforts thus far have led to the final cycle through the design cycle as previously presented in Table 15. This chapter describes the final treatment design phase, and following this, the finalized method along with the developed maturity tracker is presented and discussed.

## 6.1 Final design considerations

The findings presented in Table 19 (Chapter 5) were considered during the final design phase of this research. Although these newfound insights proved valuable, they did not necessitate the introduction of newly created activities within the aligned column of the method. Rather, they predominantly augmented the existing activities already encompassed by the methodology. Consequently, the final revision of the methodology demonstrated limited substantial changes. Instead, the novel insights presented in Table 19 were assimilated into the established activities. These findings not only validated and enriched prior knowledge but were also integrated into the pre-existing activities. Notably, the interviews consistently emphasized the significance of cultivating a culture of resilience awareness, which is widely acknowledged as a crucial component in the development of ER. Consequently, the description in the 'general governance' area of the method was expanded, and its importance was emphasized.

As described in section 5.2.2, the incorporation of a maturity tracker has been introduced to enhance the tangibility and concreteness of the method's application. The principal purpose of the maturity tracker is to enable users to assess and assign a rating to their maturity level for each activity presented in the method pertaining to the building of ER. The method presents a set of activities situated within the central column, representing a harmonious amalgamation of Risk Management activities and Information Systems Management activities. This sequence of activities, comprising proactive, intra, reactive, and general governance activities, forms the foundation for the allocation of maturity levels.

The maturity tracker encompasses an enumeration of all these aligned activities, with five distinct levels of maturity assigned to them. These levels broadly span from non-execution of the activity (maturity level 1) to proficient execution, thereby exerting a positive influence on ER (maturity level 3), and culminate in highly proficient execution, actively propelling the progress of ER at an accelerated pace (maturity level 5). The decision was made to assign a total of five maturity levels. However, levels 2 and 4 represent maturity levels in transition or in between levels, intentionally left undefined. This affords users the flexibility to assign an intermediate level when their proficiency does not align precisely with any of the predefined levels. The allocation of maturity levels is intended to facilitate users in obtaining a comprehensive overview of the activities leading to ER, facilitating the identification of areas needing improvement.

**Appendix G** provides a comprehensive overview of the allocated maturity levels for each aligned activity. The maturity tracker itself is developed using Microsoft Excel, producing a file that encompasses not only the maturity tracker but also the complete method and extensive documentation detailing the usage of ArchiMate. The goal behind this combination is to enhance the usability and accessibility of all components within a singular package. The

maturity tracker facilitates the assignment of maturity levels to individual activities using dropdown menus, enabling the calculation of the cumulative levels for all activities and the overall totals for each category. These categories are general governance, proactive, intra, and reactive activities. Consequently, this functionality empowers the user to discern areas warranting improvement through observation of the maturity level of the category. To align the method and the maturity tracker, all aligned activities were given an identification number per category (proactive, intra, reactive, and general governance).

## 6.2 Finalized method

Figure 19 illustrates the concluding iteration of the ER enhancement method in relation to the present research. Incorporating the factors outlined in the preceding section, the method has undergone multiple iterations of enhancements. These enhancements were informed by insights gathered through interviews conducted with experts in relevant domains. The final iteration of the method is further validated in Chapter 7 to ascertain its effectiveness to the fullest extent.

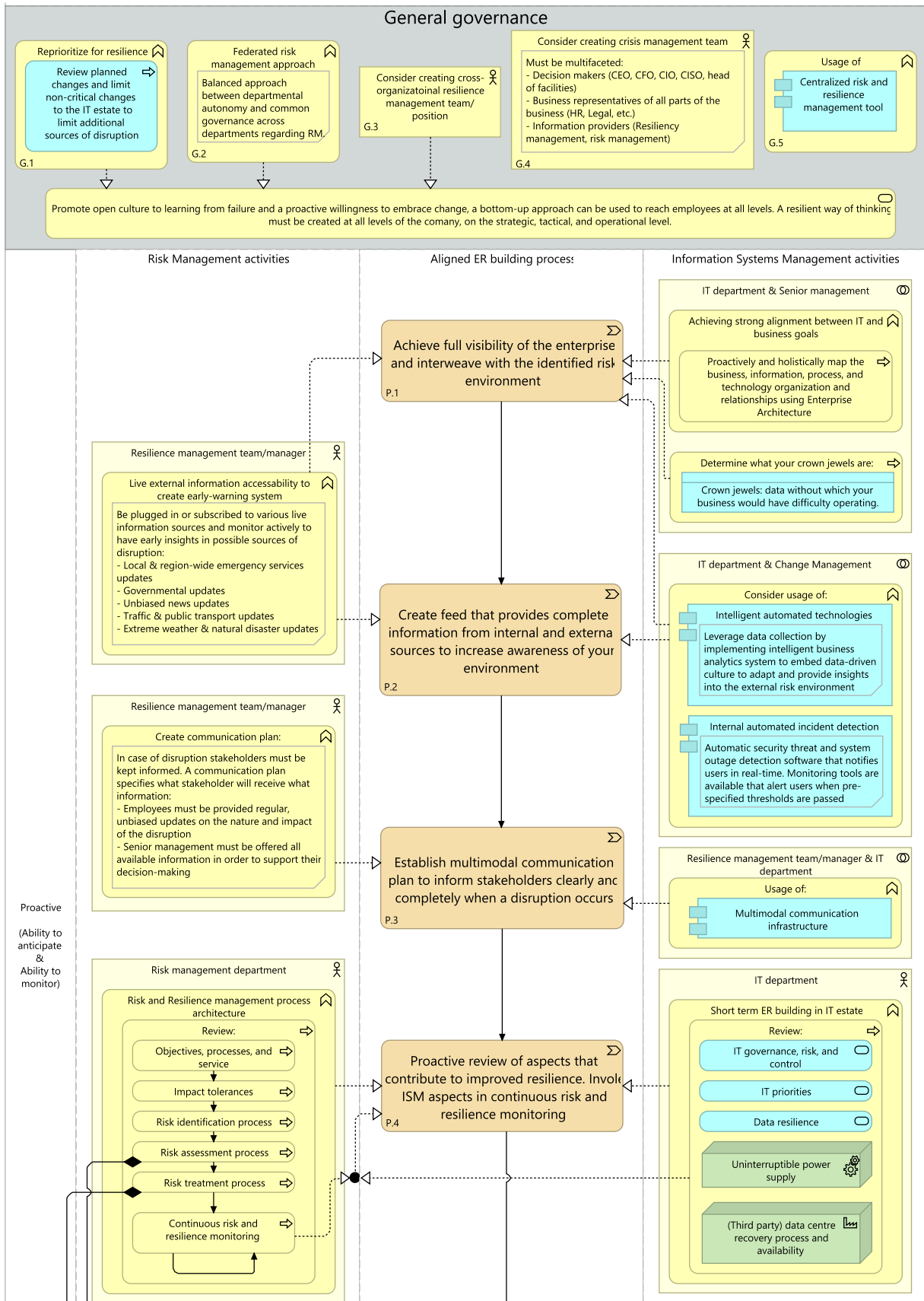
In order to enhance the comprehensibility and practicality of the method, a maturity tracker was developed depicted in Microsoft Excel. Within this spreadsheet, the final method depicted in Figure 19 is embedded. Alongside the ArchiMate specification elucidated in section 4.2.3, these components collectively constitute the comprehensive package henceforth referred to as the combined 'ER enhancement method' (See Appendix G). Consolidating all these elements enhances the usability and, consequently, the level of adoption of the method, as it is presented as an integrated entity.

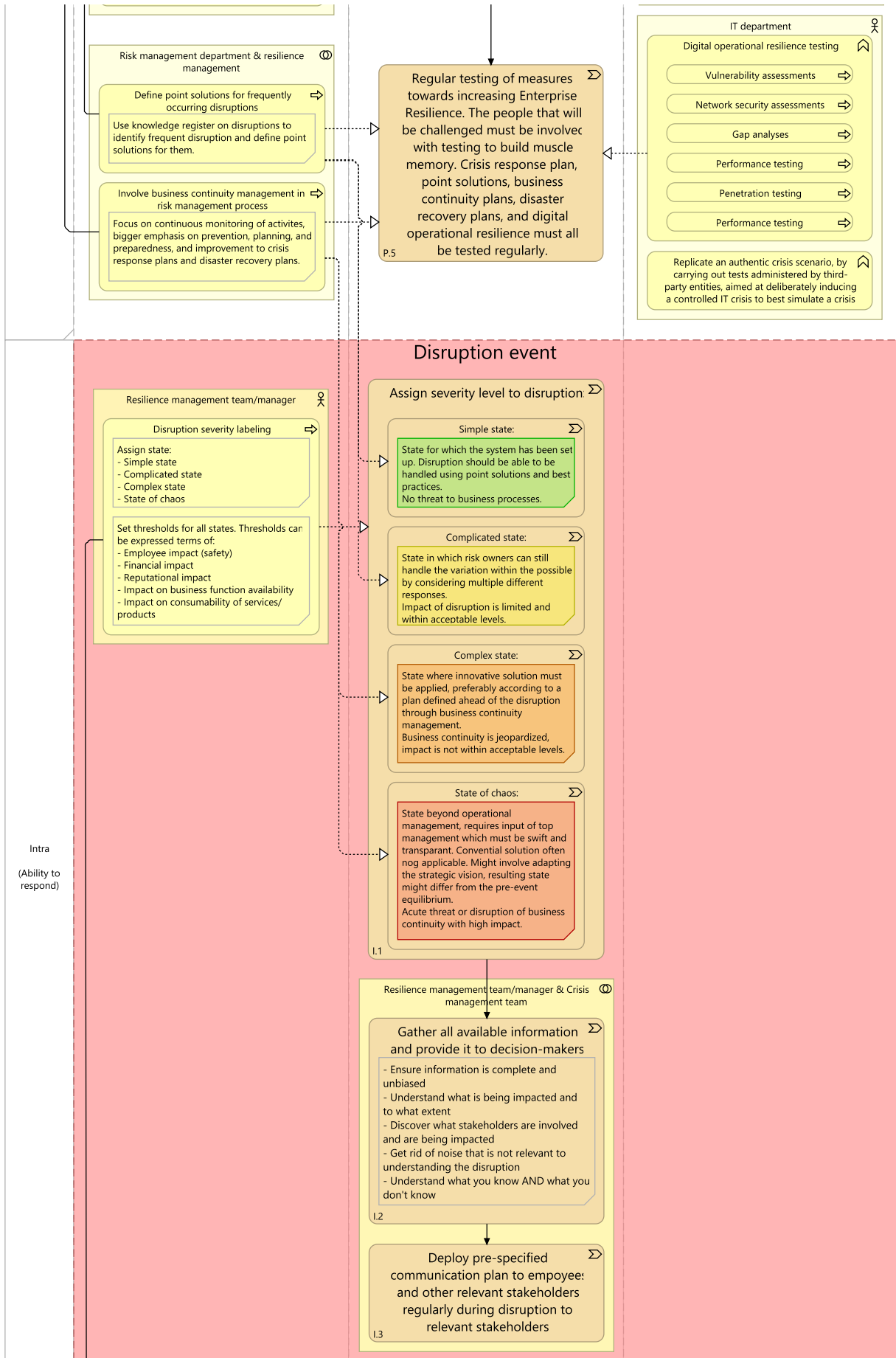
The primary objective of the ER enhancement method is to provide companies with a practical tool that facilitates the alignment of critical operational components, thereby enhancing their ER and promoting a shift towards a more resilient mindset. The method's foundation lies in its visualization, which illustrates the causal sequence of activities to be undertaken. By aligning and harmonizing essential activities from the domains of Risk Management and Information Systems Management, this causal sequence has been constructed. It is categorized into three iterative components: proactive activities, intra-disruption activities, and reactive activities. These components correspond to activities that should be performed prior to a disruption, during a disruption, and after treating a disruption, respectively. Additionally, the method incorporates activities pertaining to general governance.

To provide users of the ER enhancement method with a way of assessing their proficiency in the aligned activities, the maturity tracker was developed (Appendix G). Each activity can be assigned a maturity level, ranging from non-execution (maturity level 1) to proficient execution that positively impacts ER (maturity level 3), and culminating in highly proficient execution that actively accelerates the progress of ER (maturity level 5). By determining the maturity levels of activities, resources can accurately be allocated to areas that require improvement and attention by the firm.

This approach encourages and supports companies in actively elevating their level of ER. To validate these findings, a concluding validation phase is initiated and described in Chapter 7.

# Enterprise Resilience enhancement method





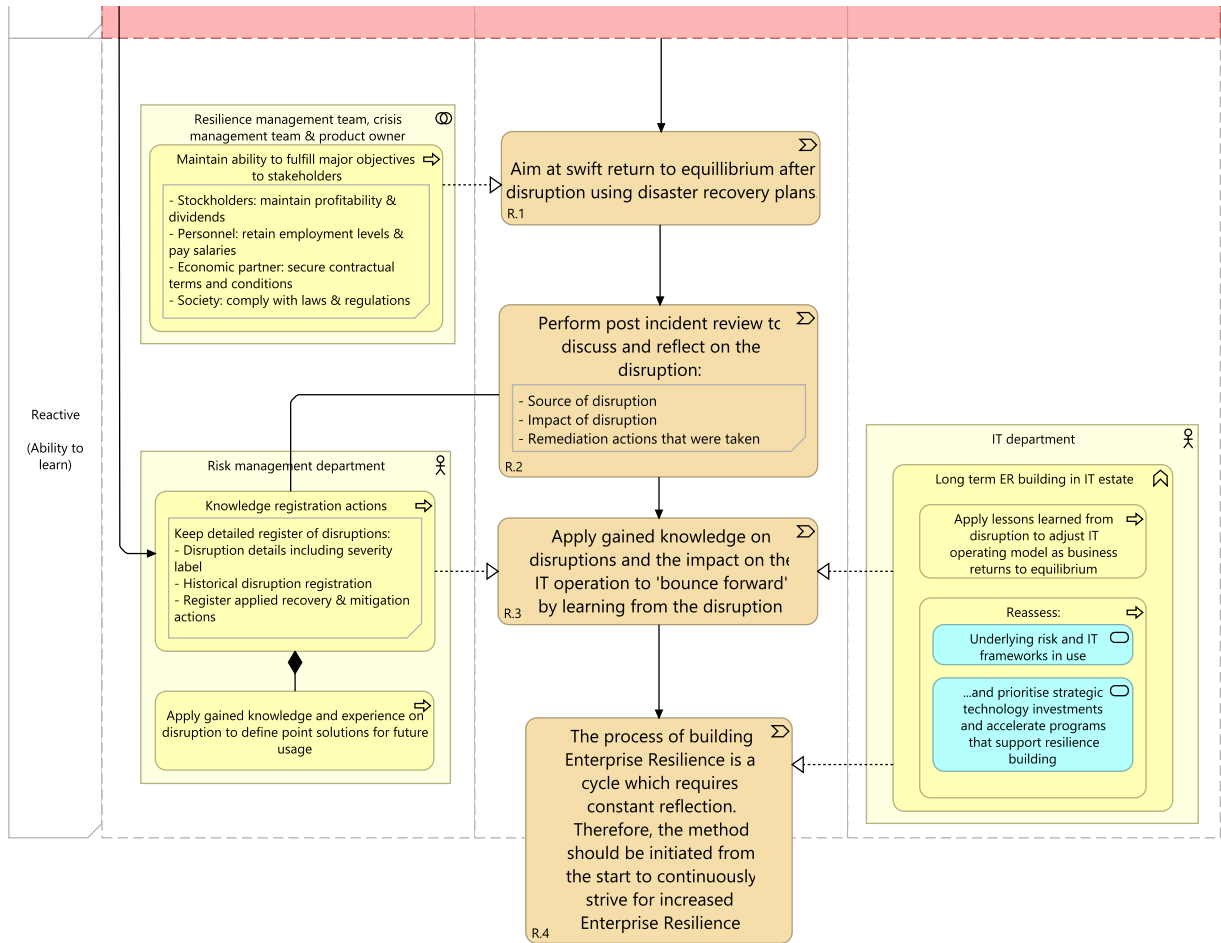


Figure 19: ER enhancement method, final edition

# 7 Validation

Chapter 7 describes the process of validating the concluding ER enhancement method presented in the previous chapter. Two instruments are utilized, a qualitative case study is executed to simulate the deployment of the method, and an evaluation of adherence to the pre-established requirements outlined in section 4.1 is performed. Through these instruments, an in-depth examination is conducted to gauge the method's effectiveness and usability. The chapter concludes with reflective insights regarding the overall performance and applicability of the method.

## 7.1 Case study

To validate the method through a qualitative case study, the approach outlined in section 4.3.2 regarding the case study is followed. This section describes the different steps that were taken and was based on the case description depicted in Appendix C. The questions asked to gather insights during the case study are depicted in Appendix D.

The case study was structured into three main components. Firstly, an interview was conducted with the participant to assess the level of ER prior to the disruptive event in order to establish a baseline. Subsequently, the researcher guided the application of the method, simulating the pre, during, and post-disruption phases. The usage of the method was then evaluated through a series of interview questions, with the objective of gathering perspectives on how the method would have influenced the company's resilience throughout the disruption. Furthermore, insights were collected regarding the usability and clarity of the method itself. Participants were selected based on the same profiles for the interview specified in Appendix A, since similar knowledge is required to execute the activities described in the method.

Table 20 presents the list of participants in the case study. The selection of these participants is based on their roles and extensive expertise in the pertinent fields. Through collaborative discussions with the participants, appropriate cases were defined, which focused on relevant situations they had encountered. This approach yielded two distinct cases that the participants possessed extensive familiarity with, in addition to being based on recent experiences. It became evident that formulating distinctive cases based on the participants' individual experiences proved more suitable than offering a choice of a predetermined set of cases that may not align with their specific profiles.

Subsequent sections provide individual descriptions of the cases, presenting a comprehensive analysis of each case study. Subsequently, detailed accounts of the results and observations derived from the case studies are provided.

*Table 20: Case study participants*

<i>Cand. ID</i>	<b>Job title</b>	<b>Years in current position</b>	<b>Company sector</b>	<b>Estimated no. of employees</b>
3.1	IT risk & compliance manager	2+ years	Financial services in pension administration	15.000+

3.2	Internal IT auditor	2+ years	Retail chain store	15.000+
-----	---------------------	----------	--------------------	---------

## 7.1.1 Case 1: Potential leak at financial services firm

### 7.1.1.1 Case description: Citrix leak

The organization referred to as ‘*Company A*’, in which Participant 3.1 was employed during the incident, is a Netherlands-based company specializing in pension administration. The case at hand revolves around a notable security breach that resulted from a breach at a third-party technology company called Citrix.

Citrix, an American cloud computing and virtualization technology company, offers a comprehensive suite of solutions including server, application, and desktop virtualization, as well as networking, SaaS, and cloud computing technologies. In 2019, Citrix publicly announced the presence of a critical vulnerability known as ‘CVE-2019-19781’<sup>3</sup> in certain software products. Specifically, vulnerabilities were found in the Citrix Application Delivery Controller. Consequently, organizations were advised to disconnect their Citrix servers. Following discussions among top management, *Company A* requested the data centre, utilized by the company, to suspend services based on the aforementioned announcement and the detection of suspicious network traffic. This decision was in alignment with the recommendations issued by the Cybersecurity and Infrastructure Security Agency (CISA) of the United States government<sup>4</sup>. As a consequence, the entire IT infrastructure of *Company A* experienced a complete outage lasting approximately six hours. This disruption was classified as a severe-level incident due to the complete unavailability of services and the inability to carry out any operational activities for a significant duration of the day.

### 7.1.1.2 Case 1: Results

The case study was executed as described in 4.3.2, thus consisting of setting a baseline in terms of the level of ER, followed by simulating the application of the method, and eventually the level of ER was measured once more as if the method were applied. As aforementioned, the level of ER is measured using a brief questionnaire developed by Hollnagel (2010). The results of this questionnaire before and after is discussed in this section, as well as the results of the application of the method.

The complete questionnaire utilized to assess the level of ER is presented in Appendix D. Table 21 displays the ratings provided by Participant 3.1, assessing the level of ER at *Company A* prior to the incident described in the preceding section. The participant was instructed to assign a level to each ability, taking into account the provided ability description and a set of supplementary questions outlined in Appendix D. The available rating options are: missing (1), deficient (2), unacceptable (3), acceptable (4), satisfactory (5), or excellent (6).

<sup>3</sup> <https://support.citrix.com/article/CTX267027/cve201919781-vulnerability-in-citrix-application-delivery-controller-citrix-gateway-and-citrix-sdwan-wanop-appliance>

<sup>4</sup> <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-031a>



Table 21: Baseline level of ER case study 1 (Hollnagel, 2010)

Essential abilities for building ER	Baseline level (1-6/Missing-Excellent)
<i>Ability to monitor</i>	4
<i>Ability to anticipate</i>	2
<i>Ability to respond</i>	3
<i>Ability to learn</i>	1

Subsequent to the aforementioned procedure, a simulation was conducted to evaluate the potential impact of implementing the method prior to the disruption. The participant was instructed to familiarize themselves with the method, gaining a comprehensive understanding of its components. Subsequently, the participant endeavoured to apply the method by completing the corresponding maturity tracker following the structure depicted in the visualization. The resulting maturity levels obtained from this exercise are presented in Appendix H, while Table 22 provides the average results per category.

Table 22: ER enhancement method; maturity tracker average results case study 1

<b>Total:</b> (Min: 17 - Max: 85)	<b>47</b>	<b>44,12%</b>
General governance total (max 25)	11	30,0%
Proactive total (max 25)	14	45,0%
Intra total (max 15)	11	66,7%
Reactive total (max 20)	11	43,8%

Following the simulation, the participant was asked to analyse their results and motivate what activities they would assign resources to for improvement. Next, based on these possible improvements, an estimation was made on the impact of the disruption and the resulting level of ER. The level of ER was once more determined using the questionnaire by Hollnagel (2010), the resulting levels and differences for each ability are presented in Table 23.

Table 23: Resulting level of ER case study 1, using Hollnagel (2010)

Essential abilities for building ER	Resulting level	Baseline Level	Difference
<i>Ability to monitor</i>	6	4	+2
<i>Ability to anticipate</i>	5	2	+3
<i>Ability to respond</i>	5	3	+2
<i>Ability to learn</i>	4	1	+3

### 7.1.1.3 Case 1: Observations

**Proactive activities:** Looking at the results of the questionnaires before and after applying the method to the Citrix leak case, it is evident that the implementation of the method led to improvements in all four essential abilities. The ability to monitor exhibited a relatively high level of maturity even prior to the application of the method. However, post-application, the participant estimated that the ability to monitor could attain the highest level of maturity classified as 'excellent'. Furthermore, there was a significant enhancement in the ability to anticipate, as observed by a three-level increase in maturity. These two abilities, monitoring and anticipation, are categorized as proactive abilities in the ER enhancement method, with a determined maturity level of 45%. This suggests a slightly below-average level of maturity in terms of monitoring and anticipating, aligning with the baseline maturity indicated by the questionnaire developed by Hollnagel (2010). It is a positive sign that no major deviations are observed in measuring the proactive aspect of ER between the questionnaire developed by Hollnagel (2010) and the ER enhancement method since this suggests the maturity tracker is an accurate tool for measuring maturity.

The participant was also asked to simulate improving the level of ER based on the usage of the method. Following this, the questionnaire was once again filled out by the participant. The consensus concerning proactive activities mainly was that the introduction of a dedicated tool, like a Security Information and Event Management (SIEM) tool, that increases awareness of the risk environment, would have had a major impact on the level of preparedness. Furthermore, *Company A* would benefit significantly from implementing a dedicated risk and resilience management process. Therefore, the result of the questionnaire regarding the ability to monitor was 'excellent' (6), and regarding the ability to anticipate was 'satisfactory' (5) in case the method was applied at *Company A*.

**Intra activities:** The initial questionnaire resulted in a maturity level of 'unacceptable' regarding the ability to respond. However, when assessing the intra activities derived from the ER enhancement method, the maturity level reached 66.7%, suggesting an above-average ability to respond. These findings exhibit a significant deviation, indicating that the set of intra activities may not be comprehensive or exhaustive. This is reflected on in the discussion (Chapter 8). The observed deviation can be partially attributed to the maturity level assigned to activity I.1 (see Appendix H). Activity I.1 pertains to the assignment of severity labels and was assigned a maximum maturity level of 5 by the participant. It is important to note that this maturity level was influenced by the mandatory requirement imposed by the Dutch government in the specific sector *Company A* resides in. Consequently, this particular activity may have introduced some bias to the overall average, as the participant acknowledged that the assigned maturity level may not have reached 5 if it were not for the enforcement requirement.

However, upon examining the disparity between the pre- and post-questionnaire responses, it becomes evident that the maturity level of the ability to respond has improved by two levels. The participant expressed the view that to a certain extent, enhancements could still be made in terms of the information-sharing protocol directed towards the relevant decision-makers (I.2), as well as a significant improvement to the sharing of information among all employees (I.3). But, a noteworthy observation was made regarding the relevance of sharing information with all employees, as it may not always be advisable to disclose all details. This cautious approach arises from the potential risks associated with causing panic among employees or the inadvertent dissemination of sensitive information to unauthorized parties. Instead, the decision to share specific information with designated individuals should be based on a careful evaluation of the nature of the disruption at hand.

**Reactive activities:** The participant initially assigned a baseline maturity level of 'missing' (1) to the ability to learn. However, upon completing the ER enhancement method, an average maturity level of 43.8% was associated with the reactive activities, which is slightly below the average. Once again, a significant discrepancy can be observed between the measured maturities. The participant noted that while some learning activities related to incidents were occasionally performed, they were not approached from a resilience perspective. Because the post-incident review process was systematically conducted and diligently stored, but this was largely due to regulatory requirements imposed on financial sector companies to do so. For this reason, they have a structured approach to post-incident reviews. However, the participant remarked that they could only assign a maturity of 4 to this activity (R.2) since this databank of post-incident reviews was rarely actually used to learn from past incidents.

Upon applying the ER enhancement method, a substantial increase of three maturity levels can be observed in the ability to learn. The participant emphasized that *Company A* has the most to gain in terms of this ability and further noted that it is also the most challenging to perfect. According to the participant, improving this ability necessitates a cultural shift towards an organization that is more conscious of resilience. Consequently, even with the enhancement of the learning activities described in the ER enhancement method, reaching a maximum maturity level of 'acceptable' (4) was deemed achievable at *Company A*.

A minor remark was made on the description of the maturity levels regarding activity R.1, since vague terms like 'long period of time' are used. Possible future iterations of the maturity tracker must address these descriptions.

**General governance:** The participant also assessed the maturity levels of the general governance activities, which initially received a significantly below-average rating of 30%. These activities do not fall under the categories of proactive, intra, or reactive, making it challenging to directly compare them with the questionnaire results. Instead, these governance activities exert influence over all the aforementioned categories, as they govern the execution of other activities. The notable low score assigned to the general governance activities offers a plausible explanation for the discrepancies observed between the ER enhancement method results and the questionnaire results. Because the absence of crucial elements in governance negatively impacts the overall organizational effectiveness in terms of ER and may therefore have skewed the results from the ER enhancement method.

#### 7.1.1.4 Case 1: Concluding remarks

In general, the participant expressed the belief that the application of the ER enhancement method would have significant positive effects on the outcome of the disruption and the level of ER at *Company A*. This sentiment is supported by the questionnaire results, which demonstrated considerable improvements in all four essential abilities. However, some disparities were observed between the maturity levels assigned through the questionnaire and those derived from the ER enhancement method. These discrepancies can be mostly attributed to the specific circumstances of the case and are described before.

It is important to note that certain activities were mandated for *Company A* by the government, indicating that not all activities may be universally applicable across different industry sectors. Consequently, a potential conclusion is that the method's scope may be too broad and would benefit from being narrowed down to fewer sectors. Furthermore, some activities may require revision in terms of their descriptions and specific details, as activities such as I.3 and R.1 were found to be somewhat lacking in clarity and completeness.

In terms of usage and clarity, the participant had no issues or remarks. The descriptions were clear and easily understood by the participant. However, it was acknowledged that individuals with less expertise in the field may find it more challenging to grasp the content. Future validation studies could help shed light on this aspect and provide further insights.

## 7.1.2 Case 2: System outage at a retail chain store

### 7.1.2.1 Case description: Warehouse management system outage

Participant 3.1, employed as an internal IT auditor at *Company B*, which operates as a retail chain store, encountered an incident during the first half of 2023. The incident pertained to a scheduled update to the warehouse management system deployed at the distribution centres of *Company B*. A warehouse management system is software that aims to streamline every part of warehouse management, from receiving and storage to picking, packing, shipping, inventory, tracking, and all steps in between. Typically, updates to this system are planned during weekends when production activities are halted. However, in this particular instance, the scheduled update exceeded the expected duration, and the warehouse management system was not operational by the time production was set to resume. Consequently, production operations were halted for half a day, impeding the distribution efforts of the company.

### 7.1.2.2 Case 2: Results

Once more, the case study consisted of setting a baseline in terms of ER, followed by simulating the application of the method and subsequently measuring the level of ER using the questionnaire developed by Hollnagel (2010). The results of this process are presented in this section. Appendix D provides a comprehensive overview of the questionnaire and additional inquiries posed during the case study. Table 24 displays the baseline levels assigned to the four fundamental abilities essential for constructing an effective ER framework. The rating options available for each ability include: missing (1), deficient (2), unacceptable (3), acceptable (4), satisfactory (5), or excellent (6).

*Table 24: Baseline level of ER case study 2 (Hollnagel, 2010)*

<b>Essential abilities for building ER</b>	<b>Baseline level (1-6/Missing-Excellent)</b>
<i>Ability to monitor</i>	4
<i>Ability to anticipate</i>	4 (close to 5)
<i>Ability to respond</i>	4
<i>Ability to learn</i>	3 (close to 4)

Subsequently, the participant was instructed to utilize the method alongside the provided maturity tracker, following a suitable period for familiarization. With the guidance of the researcher, the participant proceeded to complete the maturity tracker, and the outcomes are presented in Appendix I for reference. Moreover, the average maturity levels for each respective category are presented in Table 25 below.

Table 25: ER enhancement method; maturity tracker average results case study 2

<b>Total:</b> (Min: 17 - Max: 85)	<b>46</b>	<b>42,65%</b>
<b>General governance total (max 25)</b>	15	<b>50,0%</b>
<b>Proactive total (max 25)</b>	12	<b>35,0%</b>
<b>Intra total (max 15)</b>	8	<b>41,7%</b>
<b>Reactive total (20 total)</b>	11	<b>43,8%</b>

In conclusion, in order to evaluate the potential impact that the application of the method may have had, the participant was once again requested to complete the questionnaire regarding the four fundamental abilities essential for ER building, assuming that the method had been implemented. The outcomes of this assessment are presented in Table 26. Additionally, the participant was prompted to provide reflections on the usability and effectiveness of the method.

Table 26: Resulting level of ER case study 2, using Hollnagel (2010)

<b>Essential abilities for building ER</b>	<b>Resulting level</b>	<b>Baseline Level</b>	<b>Difference</b>
<i>Ability to monitor</i>	5	4	+1
<i>Ability to anticipate</i>	5	4 (close to 5)	+1
<i>Ability to respond</i>	5	4	+1
<i>Ability to learn</i>	4 (close to 5)	3 (close to 4)	+1

### 7.1.2.3 Case 2: Observations

**Proactive activities:** When comparing the results obtained from the questionnaire regarding proactive activities to the average maturity derived from the ER enhancement method, a discrepancy emerges. The questionnaire generally yields an approximate level of acceptable (4), while the proactive activities score below average at 35.0%. Although this presents a notable inconsistency, it is important to consider that the overall results from the questionnaire compared to the ER enhancement method appear to be skewed downwards, which may partially account for the observed disparity.

Notably, the questionnaire results demonstrate a positive difference in the abilities to monitor and anticipate, indicating a measurable enhancement in the level of ER resulting from the application of the method, as depicted in Table 26. The general conclusion from discussions with the participant was that they are in a transitional state towards a significant level of ER at *Company B*. The participant emphasized on multiple occasions that the company is actively working on improving or implementing most of the mentioned activities. In fact, *Company B* created the team participant 3.1 is a part of specifically with the goal to grow in the relevant fields. This is evident from the maturity tracker results, where many activities are rated at level 2 or 3, signifying a state of implementation that lies between a state of transition and an acceptable state. These findings align more closely with the questionnaire results, which

generally indicate an acceptable level of implementation or one close to it. Crucial activities aimed at enhancing ER are present but remain at a relatively low level of maturity, but resources are actively being allocated towards their improvement.

Furthermore, the participant highlighted that their anticipation skills are at a considerable level; however, the process itself often lacks a structured approach and relies heavily on the expertise and knowledge of key individuals. Documentation and dedicated scripts are often absent in this regard. Consequently, the participant rated the activities primarily associated with anticipation as below an acceptable level (P.3, P.4, P.5).

**Intra activities:** The application of the method, as indicated by the questionnaire results, has the potential to enhance the ability to respond. This improvement is closely linked to addressing the absence of a structured approach to crisis management and overreliance on ad-hoc solutions. For instance, *Company B* lacks a comprehensive plan to inform relevant stakeholders during a disruption (I.3), despite the participant emphasizing its importance. Although the company generally manages to navigate through disruptions due to the presence of competent individuals, the absence of documentation and a communication plan poses challenges. This also hampers the ability to conduct effective incident reflections, as there is no reference for assessing adherence to a predefined script.

Moreover, a thorough severity labelling system is missing (I.1). The participant believed some system was in place, but not well known and thus poorly executed. Overall, the participant found the intra activities worthwhile investments, since they remarked in actuality resources are currently being allocated to their improvement.

*Company B* has designated a dedicated actor responsible for gathering and disseminating information during disruptions (I.2), this has positively impacted the effectiveness of their ad-hoc crisis management. Consequently, information gathering is regarded as a highly relevant activity by the participant.

**Reactive activities:** Similar to the previous categories, the application of the method resulted in a positive impact on the ability to learn, which relates strongly to the reactive activities. This improvement was reflected in a one-level increase in the questionnaire. The participant acknowledged that enhancing this ability poses significant challenges, as it necessitates changes to established processes and measures, and the participant remarked a feedback loop on such a level is rarely successfully implemented without spending significant resources. Nonetheless, the participant recognized the value of learning from past disruptions.

In terms of returning to equilibrium (R.1), *Company B* demonstrates a general capability to do so within the available resources, leveraging the right knowledge. However, a comprehensive plan to achieve this equilibrium is still lacking. Regarding the ability to 'bounce forward' by applying lessons learned (R.3), the participant acknowledged its value but also highlighted the need for resource allocation based on the criticality of systems. For instance, systems such as warehouse management software may warrant greater investment for improvement compared to less critical systems like a declaration system. Thus, it is essential to note that the description of this activity may require further refinement in the future, as resource scarcity necessitates careful allocation in practice.

**General governance:** As previously mentioned, *Company B* is actively allocating resources towards enhancing its ER capabilities. This commitment is evident in their approach to general governance activities. Notably, they are in the process of implementing a dedicated resilience



management tool (G.5) and revamping their Risk Management approach (G.2). These initiatives have contributed to an average maturity level of 50%, which is deemed acceptable. Furthermore, these initial changes in governance lay the foundation for further development of specific proactive, intra, and reactive activities, which aligns with the goal of *Company B*. A positive conclusion can be drawn regarding the applicability of the described general governance activities, as they are currently actually being implemented by *Company B*.

#### 7.1.2.4 Case 2: Concluding remarks

Based on the overall improvement in the abilities resulting from the application of the method and the positive feedback from the participants regarding its usage and effectiveness, this case study provides confirmation of the method's usefulness in the context of the warehouse management outage case at *Company B*. The primary advantage of the method, in this case, was its emphasis on the comprehensive documentation of communication and response procedures during disruptions. Prior to experiencing the outage, *Company B* had given little attention to these aspects and had relied mostly on ad-hoc solutions to manage incidents. However, it should be noted that since the warehouse management outage case did not represent the most severe disruption, the method's effectiveness may not be as pronounced as it would be in a case of maximum severity as remarked by the participant. This is because the activities outlined in the method primarily focus on crisis mitigation and require high-level implementation, and this case was not considered a crisis by *Company B*.

Additionally, the case study revealed that *Company B* is currently in a developmental phase with respect to its ER abilities. They are actively spending resources on improvement, but they are still at an early stage. As became apparent, many of the measures they are implementing align with the activities outlined in the ER enhancement method. For this reason, the participant believed the method to be effective.

The participant concluded with a remark pertaining to the utilization of the method. Given that *Company B* possesses an internal IT & risk audit department, their expertise could potentially guide the implementation of the said methodology. However, presenting the methodology to alternative departments may pose challenges in terms of acceptance. For instance, risk managers prioritize operational activities over IT, while the IT department places less emphasis on resilience in general. Hence, the presence of a coordinating entity capable of aligning these departments becomes imperative for the effective adoption of the ER enhancement method.

## 7.2 Requirement satisfaction

A comprehensive evaluation is conducted to assess the degree of adherence to the predetermined requirements specified in section 4.1. During the preceding cycles, any deviations from complete compliance with the requirements were documented, and potential enhancements were deliberated upon. This section provides a comprehensive summary of all stipulated requirements, along with a motivation of how the final method effectively incorporates the functionality specified by these requirements. Functional requirements and their corresponding implementations are presented in Table 27, while Table 28 illustrates the implementation of non-functional requirements. The assessment of non-functional requirements is performed using the indicators defined in section 4.1.2.

The final iteration of the method demonstrates a satisfactory degree of adherence to both functional and non-functional requirements, as outlined in the respective motivations for each requirement. In this context, 'to a satisfactory degree' pertains to meeting the predefined level

of acceptance. Nevertheless, it is worth noting that several requirements could be further expanded upon in future research to achieve a more comprehensive level of fulfilment.

*Table 27: Functional requirements implementation justification*

	<b>Functional requirement</b>	<b>Motivation</b>
F1	Method must be implemented at the strategic level of a firm	All activities described are implementable at the strategic level. They are high-level activities that are implemented at the strategic level, like implementing additional measures, teams, and tools. Furthermore, overarching structures like implemented frameworks are addressed.
F2	Defines how the IT department must behave at a strategic level	In addition to the motivation for F1, specific behaviours at the strategic level regarding the IT department have been defined.
F3	Defines how IT department processes must be structured	Restructures in terms of additional processes aimed at bolstering Enterprise Resilience have been defined for the IT department. In terms of reviewing the current IT estate, additional testing for digital operational resilience, and reviewing the overarching IT governance frameworks.
F4	Defines how risk managers must behave at a strategic level	In addition to the motivation for F1, specific behaviours at the strategic level regarding the Risk Management department have been defined.
F5	Defines how Risk Management processes must be structured	Restructures in terms of additional processes aimed at bolstering Enterprise Resilience have been defined for the Risk Management department. In terms of structure the Risk Management process architecture, additional positions for building resilience, and additional positions for crisis management.
F6	Defines how collaboration between IT department processes and Risk Management processes should be arranged	The middle column in the method represents the aligned activities between the two departments. What is expected from both parties is depicted in their respective columns.
F7	Introduces holistic risk awareness across the enterprise	Promotion of a risk and resilience-aware culture can be implemented according to the method by installing a cross-organizational resilience management team that is concerned with promoting a culture open to learning from failure, risk-aware, and resilience minded.
F8	Data-driven approach, utilizing AI and BDA, allows new insights	To achieve comprehensive awareness of its entire risk environment, an organization must establish connections with appropriate external and internal information providers. The method emphasizes the utilization of data-driven instruments to effectively monitor and identify potential disruptions based on



		the collected data. By implementing this methodology, a company can enhance its ability to identify risks that might have otherwise evaded detection.
--	--	---

*Table 28: Non-functional requirements implementation justification*

	<b>Non-functional requirement</b>	<b>Motivation</b>
NF1	Must be scalable with the risk environment the firm finds itself in	During the interviews, the interviewees were asked to reflect on the effectiveness of the method in their specific risk environment. All interviewees concluded that the method potentially had at least positive effects. Therefore, the method is scalable with at least the risk environment that was analysed over the course of this research. Future testing may be necessary to confirm further risk environments.
NF2	Must be practically implementable	<p>The primary focus during the collection of activities contributing to Enterprise Resilience was on ensuring they were practically implementable. For this reason, similar available treatments and opinions from practitioners were taken as the main data sources. Moreover, the incorporation of a maturity tracker enhanced the overall comprehensibility of the package, thereby strengthening its usability and feasibility for implementation. This outcome was the result of consultations with experts in the field.</p> <p>The indicator established for NF2 was formulated based on expert opinions regarding the practicality of the approach, and subsequent consultations confirmed that the inclusion of the maturity tracker enhanced its practicality. Additionally, through interviews, the feasibility of executing all activities was assessed, leading to modifications where necessary, aimed at increasing feasibility.</p>
NF3	Must be compatible with current operations, it must fit on top of any current framework or method	While it is recommended by the method to conduct reviews of existing processes, architectures, and frameworks, the utilization of the method does not advocate for substantial modifications to these aspects. The purpose of these reviews is to assess and evaluate the organization's current state, and although they may eventually result in significant changes, immediate transformation is not a prerequisite for implementing the method. Rather, the method proposes a gradual approach through

		multiple iterations, wherein adjustments are suggested only when the current implementation proves to be ineffective. Therefore, it fits on top of current frameworks and adheres to the indicators used for validation.
NF4	Must be an iterative method that aims at continuous ER improvement	The method ends with the suggestion to immediately put focus back on monitoring and anticipating. This ensures continuous ER improvement by following the method iteratively.
NF5	Must encourage long-term growth	The ability to learn in the reactive phase is critical to encouraging long-term growth. Learning from past disruptions is encouraged over the long term, which is subsequently followed by recommencing the method through continuous monitoring and proactive anticipation. Through interviews, the importance of the ability to learn was highlighted often, which is crucial to be effective at growing over the long term. However, it was acknowledged that developing this ability presents substantial challenges, primarily due to the potential requirement of a culture shift within the organization.
NF6	Promotes distributed autonomy for departments	A federated approach towards risk and resilience management is suggested by the method. This ensures departments have the autonomy to tune their practices to their needs while following a pre-specified risk or IT framework. Moreover, no activities impose regulations on all departments, allowing for departmental autonomy. It leaves space for departmental autonomy, this validates the presence of the requirements through adherence to the indicator.

## 7.3 Validation conclusion

Two instruments were employed to validate the final iteration of the ER enhancement method. The requirement satisfaction instrument successfully verified the method's adherence to the pre-specified functional and non-functional requirements, thereby creating value for the relevant stakeholders. Consequently, the method effectively supports the stakeholders' objective of aligning Information Systems Management and Risk Management to enhance Enterprise Resilience.

Secondly, case studies were conducted to simulate the implementation of the method in diverse environments. Two distinct case studies were carried out to gather insights from different perspectives. The overall outcomes of these case studies affirmed the usability and effectiveness of the ER enhancement method, along with its accompanying maturity tracker. An independent methodology was utilized to measure potential changes in the level of Enterprise Resilience. In both case studies, a significant positive change was observed across

all key abilities essential for building Enterprise Resilience. Therefore, based on the results of these individual case studies, it can be concluded that the ER enhancement method has a positive impact on the level of ER. To bolster this claim and enhance the credibility of the method, future research could involve validation through additional case studies or, preferably, real-world implementation.

Throughout the course of the case studies, the participants noted minor observations regarding the accuracy of the description of maturity levels. However, overall, the descriptions were considered comprehensive and clear by the participants. It is expected that minor issues may arise in the current iteration of the maturity tracker, considering that it was not previously validated due to its late inclusion. Therefore, it would be beneficial for future research to revisit the descriptions and address any identified issues.

Overall, the application of the method yielded several key benefits. Firstly, it guided the process of fostering a culture that is more resilient-aware. However, it should be acknowledged that changing a culture is a complex and demanding process, and additional attention may be required in this regard. Other benefits included a heightened focus on defining proactive solutions and documenting them appropriately. Often, crisis management is carried out in an ad-hoc manner, and many organizations could benefit from increased documented response plans. Additionally, the method's continuous and iterative nature was also recognized as advantageous for instilling a resilience-aware culture throughout the entire enterprise.

---

# 8 Discussion

---

This chapter aims at discussing the results and limitations of this research and reflects on its execution. Firstly, a retrospective analysis of the employed methodologies is conducted, evaluating their applicability and efficacy. Subsequently, a critical examination of the resultant method and its associated maturity tracker is presented. This is followed by a comprehensive discussion of the limitations inherent in this research.

## 8.1 Reflection on methodology

### 8.1.1 Design Science Methodology

The Design Science Methodology proposed by Wieringa (2014) served as the foundation for the design and validation of the method employed in this research. The adoption of this methodology proved to be successful, as its structured and iterative approach facilitated the continuous enhancement of the method's efficacy with each cycle. Moreover, the detailed reporting of each cycle allows for the retrospective retracing of the design process, affirming that the method is developed in accordance with the prescribed steps outlined in the Design Science Methodology. This further strengthens the credibility of the method.

One major limitation encountered in the utilization of the Design Science Methodology within the context of this research was the inability to apply it in its entirety. The constrained scope of the research prevented the completion of the treatment implementation phase, thereby rendering it impossible to validate the method in a practical setting. Consequently, the research had to resort to simulation-based validation, which inherently fails to account for all the variables of significance in a real-world scenario. Hence, caution had to be exercised in interpreting the insights obtained from the case study. Additionally, insights on the timeline of applying the method in practice were difficult to obtain, since the method is supposed to be implemented continuously. Only very rough estimates could be gathered through interviews and case studies regarding the efficacy of the method as a continuous tool.

It is worth noting that an alternative methodology could have been considered for the design phase when the scope was defined. However, it is important to acknowledge that most alternative methodologies also rely on implementation as the primary form of validation. Therefore, adopting an alternative methodology would not have yielded significant advantages. Still, validation through implementation remains a critical aspect of future research.

### 8.1.2 Semi-structured interviews

The semi-structured interviews were conducted in accordance with the guidelines proposed by Adeoye-Olatunde and Olenik (2021). The researcher found the semi-structured interview format to be highly suitable for this research. In most instances, the flexible nature of the interview allowed for organic and open-ended conversations, while still maintaining control through guiding questions. This approach often resulted in the emergence of new topics of discussion that might not have arisen if the interview had been strictly constrained to a predefined set of questions. Although the semi-structured interview format occasionally led to interviews exceeding the allocated time, in each instance, the interviewees were willing to continue, thereby ensuring that no interviews were incomplete.

It is worth highlighting that the researcher was mostly inexperienced in conducting interviews. For this reason, there was a learning curve most likely resulting in interviews of increasing quality over time. Nevertheless, it is noteworthy that despite the researcher's relative inexperience, all interviews yielded valuable and novel insights.

Moreover, it is essential to exercise caution when interpreting the findings of qualitative interviews, as it can be challenging to completely eliminate bias from the results. In an effort to minimize bias, a diverse group of interviewees was deliberately chosen. Additionally, the iterative nature of the Design Science Methodology ensured that any potential biases introduced during the inclusion of new elements in the method were subject to expert examination in subsequent cycles. Nonetheless, it is important to acknowledge that a certain degree of bias is inevitable when conducting qualitative interviews on a limited scale.

### 8.1.3 Case study

Qualitative case studies emerged as highly suitable for the intended purpose, proving to be a more effective means of validation compared to interviews. While interviews served as robust validation tools, they also facilitated the collection of novel insights. The findings obtained from the case studies offered a greater level of detail concerning the validation of the content of the method and the maturity tracker.

One aspect of the method that posed challenges for testing through both interviews and the case study was the inclusion of a cyclic aspect to the method, which recommends users to continuously apply it. The method is designed to be implemented continuously, but even validation via a case study cannot account for this since applying the method could only be simulated once. Authentic implementation remains the sole means to thoroughly examine this aspect, which must be tested in future research. It is worth noting that different participants expressed the difficulties associated with the continuous implementation of a method over a long time, emphasizing the need for comprehensive testing in this regard.

Prior to conducting the case study, two example cases related to the COVID-19 pandemic and the Ukraine-Russia war were initially drafted. However, it soon became evident that selecting a specific case in collaboration with the participant was more appropriate. This approach ensured that the participant possessed a comprehensive understanding of the intricacies and details associated with the chosen case. Consequently, the initial example cases were discarded, and through extensive discussions with the participants, suitable cases were identified.

It is noteworthy to highlight that the two selected participants for the case studies possessed extensive knowledge and have accumulated significant experience in their respective fields. This led to an observation made by one of the participants regarding the clarity of the method for users with less expertise. They expressed that they found it easy to comprehend the concepts and intricacies of the method and the maturity tracker due to their familiarity with the subject matter. However, considering the broad range of potential users described in the scope, it becomes crucial to take into account the needs of users with varying levels of experience. Consequently, it would be valuable to conduct testing of the method with less experienced users in order to gather insights from varying perspectives.

## 8.2 Reflection on ER enhancement method

The development process of the method, encompassing design and validation phases, has been meticulously documented. This comprehensive documentation ensures that all design decisions can be retraced and their origins can be verified, thereby maximizing the credibility of the method.

Due to the extensive duration and multiple iterations involved in the design process, as well as the categorized nature of the method, the visual representation of the method (Figure 19) is vertically elongated to a significant extent. Despite efforts to mitigate this issue, the proactive, intra, and reactive categories necessitated such elongation. As a result, the size of the method may potentially impede its comprehensibility. Nevertheless, during the interviews and case studies conducted, no remarks were made regarding difficulties in comprehending the method.

Moreover, the method was not specifically scoped to any particular industry or organizational size. Based on this deliberate decision, the activities were defined in a manner that allowed for general applicability while still providing specific value. This objective was successfully achieved, and no comments were received regarding any activity being inapplicable to the tested industries or sizes. However, remarks were made concerning activities that were deemed irrelevant to certain companies because they were already mandated by the government and had reached maximum maturity already. Additionally, future testing may uncover instances where certain activities are not applicable to specific industries. Thus, these findings do not discredit the method, but careful scrutiny of applicability is advisable to adopters.

During the case studies, a discrepancy was observed regarding the varying accuracy of the maturity levels measured by the ER enhancement method and the questionnaire developed by Hollnagel (2010). As discussed in section 7.3, these discrepancies can often be explained by specific situational factors. However, it is important to note that the ER enhancement method was never intended to serve as a standalone tool for measuring the overall level of ER. Its primary purpose was to track the maturity of specific activities within the method. This implies the described activities do not encompass the entirety of activities relevant to building ER, which is a fair statement since this method is meant to develop resilience and not perfect it.

During the final validation conducted through case studies, the significance of establishing a culture that is resilient-aware was once again emphasized. However, despite the visual highlighting of the culture element within the general governance, no specific maturity level was assigned to it. This omission represents a limitation, considering that cultivating a resilient-aware culture may be one of the most pivotal aspects, albeit challenging to accomplish. Consequently, addressing this particular aspect in future iterations is imperative to enhance the comprehensiveness and effectiveness of the method.

## 8.3 Limitations

The previous reflection on the applied methodologies already revealed a few limitations of this research. As mentioned before, the Design Science Methodology had to be applied in a limited form by not executing the treatment implementation phase. Also, the limited interviewing experience may possibly have produced restricted findings. However, as outlined in the respective section, an effort was made to reduce these limitations to a minimum.

Furthermore, it is important to acknowledge that qualitative research possesses inherent limitations. One such limitation is the potential decrease in rigour concerning the credibility of the findings. Also, the substantial volume of data resulting from e.g. interview recordings, makes analysis and interpretation time-consuming, potentially leading to the loss of nuanced detail. Moreover, the presence of the researcher during data gathering may affect subjects' responses (Anderson, 2010). It is crucial to be aware of and address the limitations imposed by qualitative research. Therefore, further validation, possibly through a quantitative approach, may prove very valuable for the credibility of the method.

As highlighted during the initial design of the method, the main findings from the literature review were primarily conceptual in nature. The translation of these conceptual findings into practical activities required careful consideration. Nevertheless, the findings derived from the literature review that were incorporated into the method underwent multiple cycles of validation by expert practitioners. Any aspects deemed potentially unsuitable for practical implementation were subjected to thorough examination and modified accordingly.

While employing a case study is a viable means to validate the method, the extent of its influence within this research is constrained due to the execution of the case studies exclusively in the concluding phase. Consequently, any potential modifications to the method derived from the case study's outcomes are precluded. Nevertheless, significant insights were acquired, and the method was predominantly validated within a simulated setting. Future research could leverage the case study findings as a foundation for future redesign endeavours.

# 9 Conclusion

## 9.1 Summary & Main Conclusions

The objective of this research is to provide an answer to the primary question posed at the start of this research:

RQ1: “How to design an *alignment method* between *Information Systems Management* and *Risk Management* to achieve increased *Enterprise Resilience*, that is *practically usable* and *scaled to the risk environment* of an enterprise?”

The primary research question served as the foundational framework for this research, guiding the investigation towards a comprehensive understanding. A set of sub-questions was formulated to support and address specific dimensions of the main question. A thorough examination and subsequent responses to each of these sub-questions have contributed to the holistic response to the main research question. The answers to each sub-question are presented and discussed in detail.

### 9.1.1 Sub-Research Questions

RQ1.1: “What is *Information Systems Management* and how does it relate to Enterprise Resilience?”

Chapter 3 encompasses a comprehensive systematic literature review, with the aim of addressing RQ1.1 by examining the state-of-the-art literature pertaining to Information Systems Management and its relationship to Enterprise Resilience. Section **Fout! Verwijzingsbron niet gevonden.** delved into a detailed analysis of Information Systems Management, tracing its evolution as a recognized field of research. This evolution over the years led to the conceptualization of the updated DeLone & McLean model of Information Systems success, which considers not only the system's quality but also its utilization and the resulting net benefits. This model is considered among the most influential theories in modern IS research, leading to the definition of Information Systems Management.

This definition was formulated for Information Systems Management and was applied over the course of this research: *Information Systems Management is the usage of people and information technology and their relationships, for decision-making, coordination, and control within an organization.*

To uncover the relationship between Information Systems Management and Enterprise Resilience, a definition for Enterprise Resilience had to be determined: *Enterprise Resilience is the capacity of an enterprise, to anticipate, respond to, and be prepared for disruptive events; and the ability to continuously recover, adapt, learn, and innovate from such an event in a way that the organization emerges from it strengthened and more resourceful* (Section 3.2.1).

Information Systems Management is not always inherently related to resilience due to the risks that increasingly complex IT infrastructures bring. However, most literature suggests that Enterprise Resilience can be bolstered when Information Systems are managed in a resilient manner, these findings are presented in section 3.3. It must be supported by the right



capabilities, such as commitment, communication, competency, and coordination. Furthermore, resilient Information Systems Management can decentralize decision-making, leading to increased flexibility; an essential quality to Enterprise Resilience. Information Systems Management can be organized in an organized manner when strong alignment exists between IT and business goals. One tool that enhances visibility and facilitates this alignment is Enterprise Architecture, which enables the modelling of IT and business goals in a consolidated view.

---

RQ1.2: “What is **Risk Management** and how does it relate to Enterprise Resilience?”

The examination of Risk Management and its association with Enterprise Resilience was similarly undertaken via a systematic literature review, as detailed in Chapter 3. Given the influences of globalization, heightened technological complexity, and growing interdependencies, Risk Management has assumed an escalating significance. Consequently, organizations that lack a strategic comprehension of risk are likely to encounter difficulties in navigating uncertainty, thereby underscoring the criticality of Risk Management as a foundational element of a resilient organization (section **Fout! Verwijzingsbron niet gevonden.**).

The understanding of Risk Management obtained through the systematic literature review led to the following definition used throughout this research: *Risk Management is the identification, evaluation, and prioritization of risks followed by the application of resources to minimize, monitor, and control the effects of uncertainty on objectives.*

The prevailing perspective regarding the association between Risk Management and Enterprise Resilience is one that recognizes Risk Management as an integral component of Enterprise Resilience. Consequently, the effective implementation of Risk Management practices is expected to contribute to the enhancement of Enterprise Resilience. Section 3.4 provides an overview of the principal findings concerning this relationship. For Risk Management to effectively bolster Enterprise Resilience, it must be supported by appropriate capabilities, including risk measurement, control, and monitoring. These capabilities work in conjunction with other strategies, such as business continuity management, to reinforce Risk Management's role as a significant facilitator of Enterprise Resilience.

---

RQ1.3: “What **treatments are currently available** for achieving increased Enterprise Resilience using Information Systems Management or Risk Management?”

During the preparation of the systematic literature review, an initial observation was made, revealing the absence of explicit solutions addressing the design problem outlined in section 2.1.1. However, in order to construct the initial iteration of the ER enhancement method, it was necessary to draw upon fragments from treatments that partially addressed the design problem. By amalgamating the findings from RQ1.1 and RQ1.2, along with an exploratory search for practically focused treatments, a collection of building blocks sourced from diverse origins was defined, these are outlined in section 4.2.1, which elaborates on the chosen design approach. These building blocks originate from the systematic literature review, as well as

---

reputable entities such as KPMG, an EU regulation on digital operational resilience, and practice-focused research institutions like GRC 20/20.

---

RQ1.4: “What **enterprise qualities** lead to improved Enterprise Resilience?”

The identification of qualities that contribute to enhanced Enterprise Resilience is of utmost importance, as it provides insights into the construction of resilience and facilitates the assessment of the level of Enterprise Resilience. The availability of an instrument capable of fulfilling this role is crucial for validation purposes. Within the systematic literature review presented in Chapter 3, a diverse range of enterprise qualities leading to increased Enterprise Resilience were extracted and compiled in Table 7 (section 3.2.1.1). These qualities encompass attributes such as redundancy, robustness, flexibility, adaptive capacity, awareness, and recovery capacity.

Furthermore, four fundamental abilities critical to Enterprise Resilience were identified. These abilities—monitoring, anticipating, responding, and learning—originated from interviews with experts, as delineated in section 5.1.2.1. One of the interviewees conceptualized a resilience strategy that is currently deployed based on these abilities, which were initially articulated by Hollnagel (2010). Building upon their early findings, Hollnagel (2010) formulated a questionnaire to facilitate the straightforward measurement of Enterprise Resilience. During the validation phase of the case studies, this questionnaire was employed as a measurement instrument to acquire an impartial assessment of the participant firm's level of Enterprise Resilience (section 7.1).

---

RQ1.5: “What **stakeholders** are involved with Information Systems Management and Risk Management at the **level appropriate for improving Enterprise Resilience**, and is this the strategic, tactical, or operational level?”

During the research process, it was imperative to identify the stakeholders involved in all activities related to the development of Enterprise Resilience. However, before delving into the specific stakeholders, it was essential to determine the appropriate level at which these stakeholders operate. Section 3.2.1 of the systematic literature review unveiled that Enterprise Resilience is a capacity that encompasses the entire organization. Stakeholders aiming to enhance Enterprise Resilience must therefore operate at a level capable of influencing the organization as a whole. These strategic-level decisions are made by stakeholders at the upper management level, including the CEO, COO, CFO, CIO, and CISO. Their involvement becomes critical in times of disruption. Alongside them, representatives from various business units (e.g., HR, Legal, Facilities) and information providers must form a crisis management team that can make well-informed decisions during disruptions. Information providers can take the form of risk managers who possess an understanding of the nature of the disruption, or a dedicated resilience manager/team can be established. Moreover, this resilience manager/team holds the responsibility of cultivating a resilient-aware culture and guiding related processes. Additionally, the management of the IT department and the risk department were identified as relevant stakeholders in the context of building Enterprise Resilience. The significance of these stakeholders is elucidated in section 5.1.2.1, where the interviewees

during the development process emphasized the importance of involving people in the method. The aforementioned background knowledge regarding relevant stakeholders proved practical during the implementation of people in the method.

---

The preceding sub-questions primarily aim at acquiring knowledge and enhancing comprehension of the problem context. In contrast, questions RQ1.6-RQ1.8 pertain to the design process itself.

RQ1.6: “What are the **functional requirements** for an alignment method between Information Systems Management and Risk Management aimed at achieving increased Enterprise Resilience?”

The requirements were defined based on the desires of the identified stakeholders, ensuring the method only exhibits behaviour that creates value for the stakeholder. Relevant functional requirements were specified based on these considerations. The functional requirements are outlined in section 4.1.1, while the motivation for the finalized method’s adherence to the requirements is elucidated in section 7.2.

---

RQ1.7: “What are the **non-functional requirements** for an alignment method between Information Systems Management and Risk Management aimed at achieving increased Enterprise Resilience?”

The non-functional requirements were determined based on the same considerations as the functional requirements. However, non-functional requirements require operationalization in order to assess their fulfilment. The non-functional requirements, along with the corresponding indicators for operationalization, are outlined in section 4.1.2. The rationale behind the method's adherence to the non-functional requirements is presented in section 7.2.

---

RQ1.8: “How can an alignment method be **designed** between Information Systems Management and Risk Management to achieve increased Enterprise Resilience?”

The alignment method was designed iteratively, and according to insights gathered from validation efforts, the method was improved. The initial design was formulated by analysing available treatments and relevant literature related to the design problem following RQ1.3. This analysis resulted in a collection of activities from the fields of Information Systems Management and Risk Management, which contribute to enhancing Enterprise Resilience (section 4.2.1). An initial attempt was made to align these activities, leading to the development of the initial iteration of the method according to the chosen design dimension, which is described in section 4.2.2. To visually represent the design, the ArchiMate modelling language was adopted. The initial version of the ER enhancement method is presented in Figure 17.

The Design Science Methodology (Wieringa, 2014) outlines the various phases that should be iteratively executed to achieve reliable outcomes. Following the design phase, the resulting product needs to undergo validation. Through semi-structured interviews conducted in multiple

cycles, the method was validated. The insights obtained from these interviews were then utilized in the subsequent design phase to improve the method. During the final iteration of the design cycle, a significant design choice was made based on validation feedback, namely the inclusion of a maturity tracker for each aligned activity. This tracker enables users to assess the maturity levels of activities contributing to Enterprise Resilience, Aiming at giving them better insights into their maturity regarding resilience. The comprehensive development process is described in Chapter 5 and can be retraced in detail through extensive reporting. This extensive design process culminated in the concluding iteration of the ER enhancement method depicted in Figure 19. The accompanying maturity tracker can be found in Appendix G, along with a download link to access the combined package of these products.

---

#### RQ1.9: “How **effective** is the developed alignment method in practice?”

Testing the effectiveness of the ER enhancement method in practice had to be simulated. The Design Science Methodology was executed in a limited manner due to the fact the treatment implementation phase had to be omitted due to the limited scope of this thesis. Instead, the validation process relied on gathering insights from experts through semi-structured interviews and conducting case studies to simulate implementation. The semi-structured interviews aimed to assess the effectiveness of the method by discussing it with experts, identifying potential discrepancies with practical experiences, and confirming its effective aspects. The results from the two rounds of validation through interviews are presented in sections 5.1.2.1 and 5.2.2.1.

Additionally, to approach the highest level of validation that practical implementation offers, case studies were utilized during the final iteration of the design cycle. Collaborating with experts from diverse fields, unique cases involving significant disruptions they experienced were defined and discussed. The approach to executing the case studies is described in section 4.3.2. The case studies followed a structured process: establishing a baseline level of Enterprise Resilience prior to the disruption, simulating the application of the ER enhancement method by the participants, and measuring the level of Enterprise Resilience again to observe any changes due to the application of the method and the impact on the outcome of the disruption. The case studies served as a valuable validation instrument, as positive outcomes were observed in all cases, and the participants confirmed the method's practical applicability to real-world scenarios.

Therefore, a positive verdict can be confidently drawn regarding the effectiveness of the ER enhancement method within the bounds of the applied validation methods. However, it is imperative to validate the method through unsimulated implementation before realistic recommendations can be made regarding its adoption.

---

### 9.1.2 Primary Research Question

Having answered all sub-questions, a conclusion regarding the primary research questions can be drawn. The answers to the sub-questions previously described, fit together closely and thereby all contribute to answering the primary research question. Answering each question was essential to take the next step towards the final objective:

RQ1: “How to design an **alignment method** between **Information Systems Management** and **Risk Management** to achieve increased **Enterprise Resilience**, that is **practically usable** and **scaled to the risk environment** of an enterprise?”

The alignment method has materialized in the form of the **Enterprise Resilience enhancement method**, integrating activities from Information Systems Management and Risk Management that contribute to increased Enterprise Resilience. And thereby contributing to the goal of aligning the two aspects with the outcome of increased ER. The activities have been carefully aligned by identifying and harmonizing complementary aspects from both fields. It emphasizes the importance of a **resilience-aware culture** within organizations for achieving high maturity in Enterprise Resilience. To ensure practical relevance, the method has been shaped by setting strict requirements, gathering insights from practical frameworks, and seeking input from practising professionals. The activities and **accompanying maturity tracker** have been designed to cater to organizations operating in diverse risk environments while maintaining the necessary specificity to significantly enhance Enterprise Resilience.

The development process of the method can be retraced through the various design and validation phases, which have been thoroughly executed and documented. Multiple validation instruments have been employed to confirm the effectiveness and applicability of the method, although within the limitations of these chosen validation methods.

In practical implementation, the ER enhancement method can be adopted by following the causal aligned Enterprise Resilience building process, as presented in the visual representation of the method (Figure 19). This process outlines imperative activities for building Enterprise Resilience before, during, and after disruptions, aligning with the proactive and reactive nature of Enterprise Resilience as uncovered from the literature. The inclusion of the maturity tracker within the method serves to support and enhances tangibility. Users are able to assign maturity levels to the aligned activities, enabling them to identify areas of improvement and track their progress over time. This feature provides a valuable means of assessing and enhancing the effectiveness of the method in practice.

## 9.2 Contributions

### 9.2.1 Contributions to Science

Existing research on Enterprise Resilience and its practical improvement is limited. However, recent literature indicates a growing interest in this topic, making it a valuable area for scientific contribution. This research aims to establish the groundwork for a practical approach to constructing Enterprise Resilience, thereby filling a gap in the existing knowledge. The two fields that were selected for alignment have proven through this research to be facilitators for increasing Enterprise Resilience. By harmonising the complementing aspects of Risk Management and Information Systems Management, while also mitigating the negative influences on Enterprise Resilience through alignment, the two fields were proven to have a positive effect on the level of Enterprise Resilience.

Additionally, this research highlights the significance of cultivating a resilience-aware culture within organizations as a fundamental factor in effectively fostering Enterprise Resilience. While the importance of culture in facilitating resilience has been acknowledged in previous studies, this research emphasizes the indispensable nature of a resilience-aware culture as a

prerequisite for organizations striving for a high level of maturity in terms of Enterprise Resilience.

### 9.2.2 Contributions to Practice

The practical contribution of this research is twofold. Firstly, it presents a method for constructing Enterprise Resilience through the alignment of two commonly found fields within most organizations. By integrating these fields, the research provides a viable approach that demands minimal resources. The resulting package (Appendix G), consisting of the Enterprise Resilience enhancement method and the accompanying maturity tracker, offers a tangible and accessible framework that organizations can readily implement alongside their existing structures.

Secondly, this study incorporates an evaluation conducted with industry experts specializing in Risk Management, Information Technology, and resilience. The positive evaluation of the proposed method by these practitioners establishes it as a valuable guideline for practical implementation. As a result, this research serves as a valuable resource for practitioners seeking effective strategies to enhance Enterprise Resilience.

A design objective was to ensure practical implementation, thereby departing from the predominantly conceptual nature of existing Enterprise Resilience research. By following this design philosophy and confirming the resulting findings with practising experts, the practicality, usability, and feasibility have remained critical targets and this is reflected in the concluding iteration of the ER enhancement method.

## 9.3 Future work

Rigorous validation endeavours have been undertaken to affirm the credibility of the ER enhancement method. However, the utilization of case studies in a concluding validation capacity without subsequent design phases has naturally unveiled certain unaddressed limitations. Section 7.3 discusses minor findings stemming from these case studies, which necessitate attention in potential future iterations. The iterative nature of the Design Science Methodology provides the opportunity for ongoing development in subsequent research. By meticulously documenting the development efforts up to the present stage, future investigations can continue the advancement process.

In the context of this research, two case studies were conducted, yielding positive outcomes with respect to the effectiveness of the proposed method. However, it is crucial to acknowledge the significantly limited number of case studies employed. Future research should consider conducting case studies in diverse contexts encompassing varying company sizes, sectors, and different risk environments. Moreover, two cases were pre-defined regarding the COVID-19 pandemic, and the Ukraine-Russia war, representing disruptions of the utmost severity. Exploring how different companies would have experienced these events had the ER enhancement method been applied, may offer novel perspectives on the efficacy of the method.

With the method validated through additional case studies, its readiness for implementation becomes increasingly apparent. Practical implementation and subsequent impact assessment serve as the ultimate validation instruments. Therefore, future endeavours should focus on real-life implementation to conclude the validation process.

A crucial requirement for the method was its design to facilitate seamless integration into existing organizational structures. This approach has resulted in a more feasible and tangible product, considering the fact Enterprise Resilience is a developing capacity in literature, and must therefore be introduced gradually. However, future research can utilize the findings of this study to conceptualize a dedicated resilience framework that encompasses all aspects of the organization. Such a framework would interconnect various elements of the company in a resilient manner, addressing the entirety of the organization's operations and functions.

# 10 Bibliography

- Adeoye-Olatunde, O. A., & Olenik, N. L. (2021). Research and scholarly methods: Semi-structured interviews. *Journal of the American College of Clinical Pharmacy*, 4(10), 1358-1367.
- Al-Kofahi, M. K., Hassan, H., Mohamad, R., Intan, T., & Com, M. (2020). Information systems success model: A review of literature. *International Journal of Innovation, Creativity and Change*, 12(8).
- Alawamleh, H. A., Alshibly, M. H. A.-a., Tommalieh, A. F. A., Al-Qaryouti, M. Q. H., & Ali, B. (2021). The challenges, barriers and advantages of management information system development: Comprehensive review. *Academy of Strategic Management Journal*, 20(5), 1-8.
- Aldea, A., Vaicekaskaitė, E., & Daneva, M. (2020). Assessing resilience in enterprise architecture: a systematic review. *2020 IEEE 24th ....*
- Allen, J. H., & Davis, N. (2010). Measuring operational resilience using the cert resilience management model.
- Anderson, C. (2010). Presenting and evaluating qualitative research. *American journal of pharmaceutical education*, 74(8).
- APQC. (2011). How to First Adopt, Then Adapt Process Frameworks and Models.
- Assibi, A. T. (2022). The Role of Enterprise Risk Management in Business Continuity and Resiliency in the Post-COVID-19 Period. *Open Access Library Journal*, 9(6), 1-19.
- Bak, O., Shaw, S., Colicchia, C., & Kumar, V. (2023). A Systematic Literature Review of Supply Chain Resilience in Small-Medium Enterprises (SMEs): A Call for Further Research. *IEEE Transactions on Engineering Management*, 70(1), 328-341. doi:10.1109/TEM.2020.3016988
- Barroso, A. P., Machado, V. H., & Machado, V. C. (2008). *A supply chain disturbances classification*. Paper presented at the 2008 IEEE International Conference on Industrial Engineering and Engineering Management.
- Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *The qualitative report*, 13(4), 544-559.
- Buganová, K., Mošková, E., & Šimíčková, J. (2021). Increasing the Resilience of Transport Enterprises through the Implementation of Risk Management and Continuity Management. *Transportation Research Procedia*, 55, 1522-1529. doi:10.1016/j.trpro.2021.07.141
- Ciampi, F., Marzi, G., & Rialti, R. (2018). Artificial intelligence, big data, strategic flexibility, agility, and organizational resilience: A conceptual framework based on existing literature.
- Conz, E., & Magnani, G. (2020). A dynamic perspective on the resilience of firms: A systematic literature review and a framework for future research. *European Management Journal*, 38(3), 400-412. doi:10.1016/j.emj.2019.12.004
- D'arcy, S. P., & Brogan, J. C. (2001). Enterprise risk management. *Journal of Risk Management of Korea*, 12(1), 207-228.
- DeLone, W. H., & McLean, E. R. (1992). Information systems success: The quest for the dependent variable. *Information systems research*, 3(1), 60-95.
- DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: a ten-year update. *Journal of management information systems*, 19(4), 9-30.
- Ennouri, W. (2013). Risks management: new literature review. *Polish journal of management studies*, 8, 288-297.
- Erol, O., Sauser, B., & Mansouri, M. (2010). A framework for investigation into extended enterprise resilience. *Enterprise Information Systems*. doi:10.1080/17517570903474304



- Fiksel, J. (2016). The new resilience paradigm-essential strategies for a changing risk landscape i. *IRGC Resource Guide on Resilience*, 1-5.
- Gomes, R. (2015). Resilience and enterprise architecture in SMEs. *JISTEM-Journal of Information Systems and Technology Management*, 12, 525-540.
- Grace, M. F., Leverty, J. T., Phillips, R. D., & Shimpi, P. (2015). The value of investing in enterprise risk management. *Journal of Risk and Insurance*, 82(2), 289-316.
- GRC 20/20 Research. (2022). Risk & Resiliency Management by Design: An Integrated Approach to Risk & Resilience Management.
- Hamel, G., & Valikangas, L. (2004). The quest for resilience. *icade. Revista de la Facultad de Derecho*(62), 355-358.
- Hassan, Y., Kushwaha, A., & Sharma, V. (2022). Organizational resilience through techno-structural interventions: case of an Indian wealth management firm. *International Journal of Law and Management*. doi:10.1108/IJLMA-03-2022-0049
- Heeks, R., & Ospina, A. V. (2019). Conceptualising the link between information systems and resilience: A developing country field study. *Information Systems Journal*, 29(1), 70-96. doi:10.1111/isj.12177
- Hepfer, M., & Lawrence, T. (2022). The Heterogeneity of Organizational Resilience: Exploring functional, operational and strategic resilience. *Organization Theory*. doi:10.1177/26317877221074701
- Hollnagel, E. (2010). *How resilient is your organisation? An introduction to the resilience analysis grid (RAG)*. Paper presented at the Sustainable transformation: Building a resilient organization.
- Hollnagel, E. (2013). *Resilience engineering in practice: A guidebook*: Ashgate Publishing, Ltd.
- Hopkin, P. (2018). *Fundamentals of risk management: understanding, evaluating and implementing effective risk management*: Kogan Page Publishers.
- Hubbard, D. W. (2020). *The failure of risk management: Why it's broken and how to fix it*: John Wiley & Sons.
- Hudakova, M., & Lahuta, P. (2020). Risk Management as a Tool for Building a Resilient Enterprise. *Economic and Social Development: Book of Proceedings*, 248-258.
- Ignatiadis, I., & Nandhakumar, J. (2007). The impact of enterprise systems on organizational resilience. *Journal of Information Technology*, 22(1), 36-43. doi:10.1057/palgrave.jit.2000087
- International Organization for Standardization. (2017). Security and resilience - Organizational resilience - Principles and attributes (ISO Standard No. 22316:2017). Retrieved from <https://www.iso.org/standard/50053.html>
- International Organization for Standardization. (2018). Risk management - Guidelines (ISO Standard No. 31000:2018). Retrieved from <https://www.iso.org/standard/65694.html>
- Keen, P. G. W. (1980). *Mis Research: Reference disciplines and a Cumulative Tradition*. Paper presented at the International Conference on Interaction Sciences.
- Kitchenham, B., & Charters, S. (2007). Guidelines for performing Systematic Literature Reviews in Software Engineering. 2.
- KPMG. (2020). COVID-19: A guide to maintaining Enterprise Resilience. Retrieved from <https://assets.kpmg.com/content/dam/kpmg/ph/pdf/Enterprise%20Resilience%20Framework.pdf>
- Lengnick-Hall, C. A., Beck, T. E., & Lengnick-Hall, M. L. (2011). Developing a capacity for organizational resilience through strategic human resource management. *Human resource management review*, 21(3), 243-255.
- Lisdiono, P., Said, J., Yusoff, H., & Hermawan, A. A. (2022). Risk management practice, alliance management capability, and enterprise resilience: Findings from Indonesian state-owned enterprises. *Problems and Perspectives in Management*, 20(1), 190-202. doi:10.21511/ppm.20(1).2022.17
- Louisot, J.-P. (2015). Risk and/or resilience management. *RISK GOVERNANCE & CONTROL: Financial markets and institutions*, 5(2), 84-91.

- Madani, F., & Parast, M. M. (2023). An integrated approach to organizational resilience: a quality perspective. *International Journal of Quality and Reliability Management*, 40(1), 192-225. doi:10.1108/IJQRM-07-2020-0229
- Madni, A. M., & Jackson, S. (2009). Towards a conceptual framework for resilience engineering. *IEEE Systems Journal*, 3(2), 181-191.
- Mallach, E. G. (2015). *Information Systems: What Every Business Student Needs to Know*.
- Mallak, L. A., & Yildiz, M. (2016). Developing a workplace resilience instrument. *Work*, 54(2), 241-253.
- McManus, S., Seville, E., Vargo, J., & Brunson, D. (2008). Facilitated process for improving organizational resilience. *Natural Hazards Review*, 9(2), 81-90. doi:10.1061/(ASCE)1527-6988(2008)9:2(81)
- Ni, H., Chen, A., & Chen, N. (2010). Some extensions on risk matrix approach. *Safety Science*, 48(10), 1269-1278.
- Oh, L.-B., & Teo, H.-H. (2009). An empirical study of IT-enabled enterprise risk management and organizational resilience.
- Orlikowski, W. J. (1991). Integrated information environment or matrix of control? The contradictory implications of information technology. *Accounting, management and information technologies*, 1(1), 9-42.
- Pal, R., Torstensson, H., & Mattila, H. (2014). Antecedents of organizational resilience in economic crises - An empirical study of Swedish textile and clothing SMEs. *International Journal of Production Economics*, 147(PART B), 410-428. doi:10.1016/j.ijpe.2013.02.031
- Pettit, T. J., Fiksel, J., & Croxton, K. L. (2010). Ensuring supply chain resilience: development of a conceptual framework. *Journal of business logistics*, 31(1), 1-21.
- Pettit, T. J., Fiksel, J., Polyviou, M., & Croxton, K. (2014). *Embracing Change: From Risk to Resilience*. Retrieved from
- Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations, OJ L333 C.F.R. (2022).
- Rohmeyer, P., & Zvi, T. B. (2009). *Risk management decision making in ICT for development*. aisel.aisnet.org.
- Sanchis, R., Canetta, L., & Poler, R. (2020). A conceptual reference framework for enterprise resilience enhancement. *Sustainability (Switzerland)*, 12(4). doi:10.3390/su12041464
- Sanchis, R., & Poler, R. (2014). Enterprise resilience assessment: A categorisation framework of disruptions. *Direccion y Organizacion*, 54, 45-53.
- Schemmer, M., Heinz, D., Baier, L., Vössing, M., & Köhl, N. (2021). *Conceptualizing Digital Resilience for AI-based Information Systems*: researchgate.net.
- Schinagl, S., Shahim, A., Khapova, S., & Van Den Hooff, B. (2023). Digital Security Governance: What Can We Learn from High Reliability Organizations (HROs)?
- Seddon, P. B. (1997). A respecification and extension of the DeLone and McLean model of IS success. *Information systems research*, 8(3), 240-253.
- Sheth, A., & Kusiak, A. (2022). Resiliency of Smart Manufacturing Enterprises via Information Integration. *Journal of Industrial Information Integration*, 100370.
- Sin, I., & Ng, K. (2013). *The evolving building blocks of enterprise resilience: ensnaring the interplays to take the helm*: academia.edu.
- Skulimowski, A., & Łydek, P. (2022). *Applications of AI Alignment and Anticipatory Networks to Designing Industrial Risk Management Decision Support Systems*: aisel.aisnet.org.
- Taylor, L. (2014). *Practical enterprise risk management: How to optimize business strategies through managed risk taking*: Kogan Page Publishers.
- Teece, D., Peteraf, M., & Leih, S. (2016). Dynamic capabilities and organizational agility: Risk, uncertainty, and strategy in the innovation economy. *California management review*, 58(4), 13-35.
- Teoh, S. Y., & Zadeh, H. S. (2013). *Strategic resilience management model: Complex enterprise systems upgrade implementation*.
- The Institute of Internal Auditors. (2020). The IIA's three lines model.

- The Open Group. (2023). ArchiMate® 3.2 Specification. Retrieved from [https://pubs.opengroup.org/architecture/archimate32-doc/archimate\\_3\\_2\\_specification.html](https://pubs.opengroup.org/architecture/archimate32-doc/archimate_3_2_specification.html)
- Thiede, M., Fuerstenau, D., & Bezerra Barquet, A. P. (2018). How is process mining technology used by organizations? A systematic literature review of empirical studies. *Business Process Management Journal*, 24(4), 900-922.
- To, H., & Teer, J. (2020). COVID-19: A guide to maintaining Enterprise Resilience.
- Tuncel, G., & Alpan, G. (2010). Risk assessment and management for supply chain networks: A case study. *Computers in industry*, 61(3), 250-259.
- Velu, S. R., Al Mamun, A., Kanesan, T., Hayat, N., & Gopinathan, S. (2019). Effect of information system artifacts on organizational resilience: A study among Malaysian SMEs. *Sustainability (Switzerland)*, 11(11). doi:10.3390/su111113177
- Wang, D., & Chen, S. (2022). Digital Transformation and Enterprise Resilience: Evidence from China. *Sustainability (Switzerland)*, 14(21). doi:10.3390/su142114218
- Wang, N., Cui, D., & Jin, C. (2023). The Value of Internal Control during a Crisis: Evidence from Enterprise Resilience. *Sustainability*, 15(1), 513.
- Wieringa, R. J. (2014). *Design science methodology for information systems and software engineering*: Springer.
- Winston, A. (2014). Resilience in a hotter world. *Harvard business review*, 92(4), 56-64, 132.
- Woods, D., & Wreathall, J. (2003). Managing risk proactively: The emergence of resilience engineering. *Columbus: Ohio University*.
- Xu, D., Tsang, I. W., Chew, E. K., Siclari, C., & Kaul, V. (2019). A data-analytics approach for enterprise resilience. *IEEE Intelligent Systems*, 34(3), 6-18.

---

# 11 Appendix

---

## Appendix A: Desired interviewee profiles

### Profiles:

- Resiliency Expert:
  - o Possesses expertise in developing resilience within an organization.
  - o Knowledgeable in operational resilience, organizational resilience, and/or financial resilience.
- Risk Management Expert:
  - o Familiarity with traditional proactive risk management approaches.
    - Proficient in managing risks across both financial and non-financial domains.
  - o Preferably experienced in crisis management.
  - o Preferably knowledgeable in Enterprise Resilience.
  - o Preferably actively engaged in a firm that actively manages resilience.
- IT Governance/Risk Expert:
  - o Proficient in managing IT strategy within an organization.
  - o Proficient in managing IT risk.
  - o Preferably familiar with Enterprise Resilience.
  - o Preferably knowledgeable in harnessing the potential of IT.
  - o Preferably actively involved in a firm that actively manages resilience.

### General Preferences:

- Participants with at least five years of active experience in their respective roles.
- Participants capable of participating in interviews conducted in English.

## Appendix B: Interview Questions

### ***Part 1: Relationships between Information Systems Management and Enterprise Resilience & Risk Management and Enterprise Resilience***

- Do you consent to the results of this interview being used for my research? Your personal data will be processed and presented only in such a way that you remain anonymous.
- Do you consent to the audio of this interview being recorded, purely for scientific purposes? All recordings will be erased after they are processed.
  
- What is your job description and what does it entail?
  - Title
  - Years of experience
  - Company sector
  - Number of employees

#### **Enterprise Resilience:**

- Does your company concern itself with Enterprise Resilience (or other forms of resilience), and in what way?
  
- Do you feel Enterprise Resilience is an important capacity for companies to possess and why?
  
- Do you believe your company is adequately concerned with Enterprise Resilience and why?
  
- Can you name any processes or functions in your company that lead to increased Enterprise Resilience?
  
- What qualities must companies possess in order to achieve Enterprise Resilience?

#### **Risk Management and Enterprise Resilience:**

- How do Risk Management and Enterprise Resilience differ in your experience?
  
- Do you believe Risk Management activities can be leveraged to support building Enterprise Resilience and in what way?
  
- Do you believe increasing focus on Enterprise Resilience can have negative effects on established processes? For example, Risk Management processes or others?

- When a disruption occurs, is it labelled in a certain way? (e.g. on severity?) And are the disruptions registered or archived?

**Information Systems Management and Enterprise Resilience:**

- How do you view the relationship between Information Systems Management and Enterprise Resilience?
- Do you believe Information Systems Management can be an enabler for increasing Enterprise Resilience and in what way?
- Do you believe Information Systems Management can negatively influence the level of Enterprise Resilience and in what way?
- In what ways can Information Systems Management and Risk Management be aligned to achieve Enterprise Resilience?

***Part 2: Initial method discussions***

- Are you familiar with the Enterprise Architecture modelling language ArchiMate?
- Open discussion about model
  - Adoptability of methods/framework?
  - Is the distinction between proactive, intra, and reactive valid in your opinion?

## Appendix C: Case description (Example: COVID-19)

**Approximate duration:** 1 hour

**Data will be anonymized**

- 1) **Introduction:** In this case study, I aim to examine the impact of a method designed to enhance Enterprise Resilience in the face of unforeseen challenges, focusing on the COVID-19 pandemic. The study involves a participant from a company who will be asked to apply the method retrospectively, as if it were before the pandemic. Through a series of interviews and analysis, we will gather insights into how the application of this method could have influenced the company's Enterprise Resilience during the COVID-19 crisis.
- 2) **Background:** The COVID-19 pandemic has posed unprecedented challenges to businesses worldwide, disrupting operations, supply chains, and market dynamics. Many organizations struggled to adapt to the rapidly changing environment, while others demonstrated remarkable resilience by navigating the crisis successfully. Enterprise Resilience, the ability of an organization to anticipate, respond, and recover from disruptive events, plays a crucial role in determining long-term sustainability and competitiveness.
- 3) **Research Objectives:** The primary objective of this case study is to assess the effectiveness of a method aimed at improving Enterprise Resilience during the COVID-19 pandemic. The study seeks to:
  - a) Understand the baseline Enterprise Resilience of the participating company prior to the pandemic.
  - b) Evaluate the application of the method by the participant, considering its potential impact on the company's Enterprise Resilience.
  - c) Gather insights and lessons learned from the participant's experience to refine and enhance the method for future use.
- 4) **Methodology:** The case study will follow a sequential process, consisting of the following key steps:
  - a) **Baseline Assessment:**
    - i) Conduct interview and gather information about the company's pre-pandemic operations, strategies, and capabilities.
    - ii) Assess the company's existing Enterprise Resilience, focusing on the abilities to monitor, anticipate, respond, and learn from disruption.
  - b) **Method Application:**
    - i) Provide the participant with the developed method and instruct them to apply it retrospectively, as if it were before the pandemic.
    - ii) The participant will be guided through the implementation process, making relevant decisions and adjustments based on their understanding of the method and the company's specific context.
  - c) **Insights and Evaluation:**
    - i) Conduct interview after the application with the participant to gather their perspectives on how the method would have impacted the company's resilience during the COVID-19 crisis.
    - ii) Analyse the participant's responses and identify key insights regarding the effectiveness of the method, potential areas of improvement, and lessons learned.



- 5) **Expected Outcomes:** By the end of this case study, we anticipate the following outcomes:
  - a) Assessment of Baseline Resilience:
    - i) An understanding of the company's Enterprise Resilience strengths and weaknesses before the pandemic.
    - ii) Identification of any pre-existing measures that contributed to the company's ability to navigate the crisis.
  - b) Method Impact Evaluation:
    - i) Insights into how the application of the method would have influenced the company's Enterprise Resilience during the COVID-19 pandemic.
    - ii) Identification of specific aspects of the method that proved beneficial or required further refinement.
  - c) Lessons Learned and Recommendations:
    - i) Key takeaways and lessons learned from the participant's experience, providing valuable insights for enhancing the method's efficacy.
    - ii) Recommendations for improving the ER enhancement method in the future.
- 6) **Conclusion:** This case study presents an opportunity to retrospectively evaluate the impact of a method aimed at improving Enterprise Resilience during the COVID-19 pandemic. By analysing the participant's application of the method, we will gain valuable insights into its effectiveness, enabling organizations to enhance their preparedness and adaptability in the face of future challenges.

## Appendix D: Case study questions

Notes:

- Some aspects of the questionnaire or the method might be outside the scope of what the participant is concerned with within their company, these questions will not be taken into account in the results of the case study. In a real situation, the relevant stakeholder to that aspect may be involved to address such an issue.
- The activities will be assigned a maturity level by the participant. The follow-up question is: would you raise the maturity level of each activity?
  - o Yes; to what level and what resources would be spent?
  - o No; why not? Not worth the resources? Not an effective measure?

### **Determining the baseline Enterprise Resilience ahead of the occurrence of the disruption**

An overall assessment of the organization's degree of resilience can be made using the questionnaire by Hollnagel (2010). The brief questionnaire allows the evaluation of the four key abilities essential to resilience; the ability to monitor, anticipate, respond, and learn.

This alternative Enterprise Resilience maturity model is used to set a baseline that is not influenced by the method itself.

**The ability to monitor:** How well is the organisation able to detect smaller or larger changes to work conditions (internal and/or external) that may affect the organisation's ability to carry out current or intended operations?

Excellent	Satisfactory	Acceptable	Unacceptable	Deficient	Missing

The rating of this ability can be helped by asking some more detailed questions, for instance:

- How does the organization monitor the situation and how are the indicators defined?
- How is the validity of the indicators established?
- How are the 'readings' used and communicated?

**The ability to anticipate:** How large an effort does the organisation put into what may happen in the near future? Is anticipation a strategic concern?

Excellent	Satisfactory	Acceptable	Unacceptable	Deficient	Missing

The rating of this ability can be helped by asking some more detailed questions, for instance:

- How does the organization (or people in charge) think about the future? What is the 'model of the future' that the organization uses?
- How long is the organization's time horizon (for instance, number of years)?
- How is the cost-benefit of investments in the future established?

**The ability to respond:** How ready is the organisation to respond and how able (quickly and efficiently) is it to respond when something unexpected happens?

Excellent	Satisfactory	Acceptable	Unacceptable	Deficient	Missing

The rating of this ability can be helped by asking some more detailed questions, for instance:

- How complete is the set of events for which the organization is ready to respond?
- How fast can a response be given and how long can it be sustained?
- How is the readiness to respond ensured and maintained?

**The ability to learn:** How well does the organisation make use of formal and informal opportunities to learn from what happened in the past?

Excellent	Satisfactory	Acceptable	Unacceptable	Deficient	Missing

The rating of this ability can be helped by asking some more detailed questions, for instance:

- How selective is the basis for learning? Does the organization consider both failures and successes?
- How often does the organization try to learn? Continuously or when something has happened?
- How is learning expressed? (rules, procedures, attitudes, skills, etc.)?

### ***Evaluate the potential impact on Enterprise Resilience by applying the method***

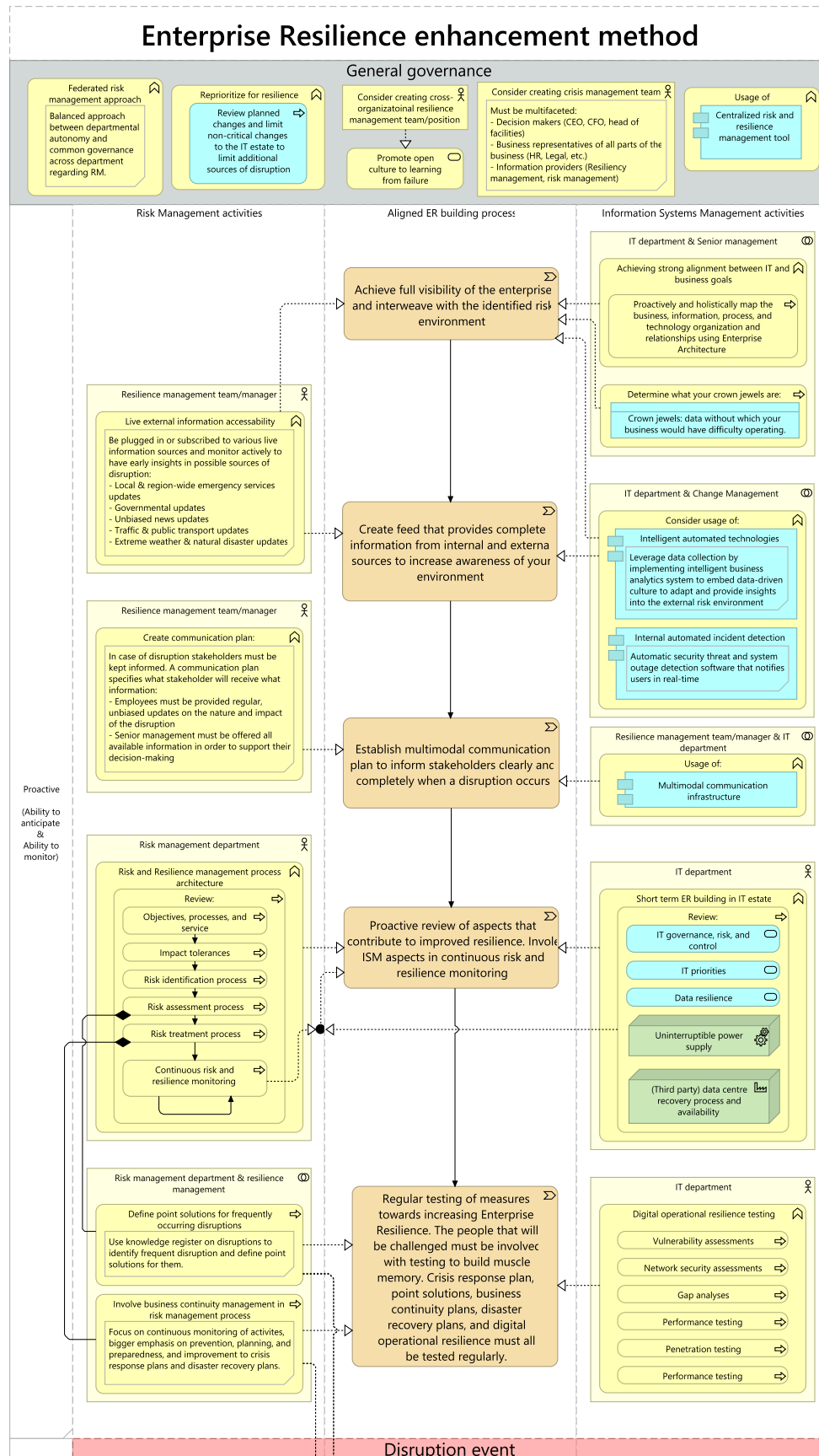
- The activities will be assigned a maturity level by the participant. The follow-up question is: would you raise the maturity level of each activity?
  - o Yes; to what level and what resources would be spent?
  - o No; why not? Not worth the resources? Not an effective measure?
- *Again, use the questionnaire defined by Hollnagel (2010) to determine any possible changes in the maturity in any of the abilities.*
- Do you believe applying the method would have allowed you to handle with the disruption better?
- What impact do you believe applying the method would have had on your level of Enterprise Resilience?
- Do you believe applying the method introduces any benefits, and what would these be?
- Do you believe applying the method leads to any negative effects, and what would these be?

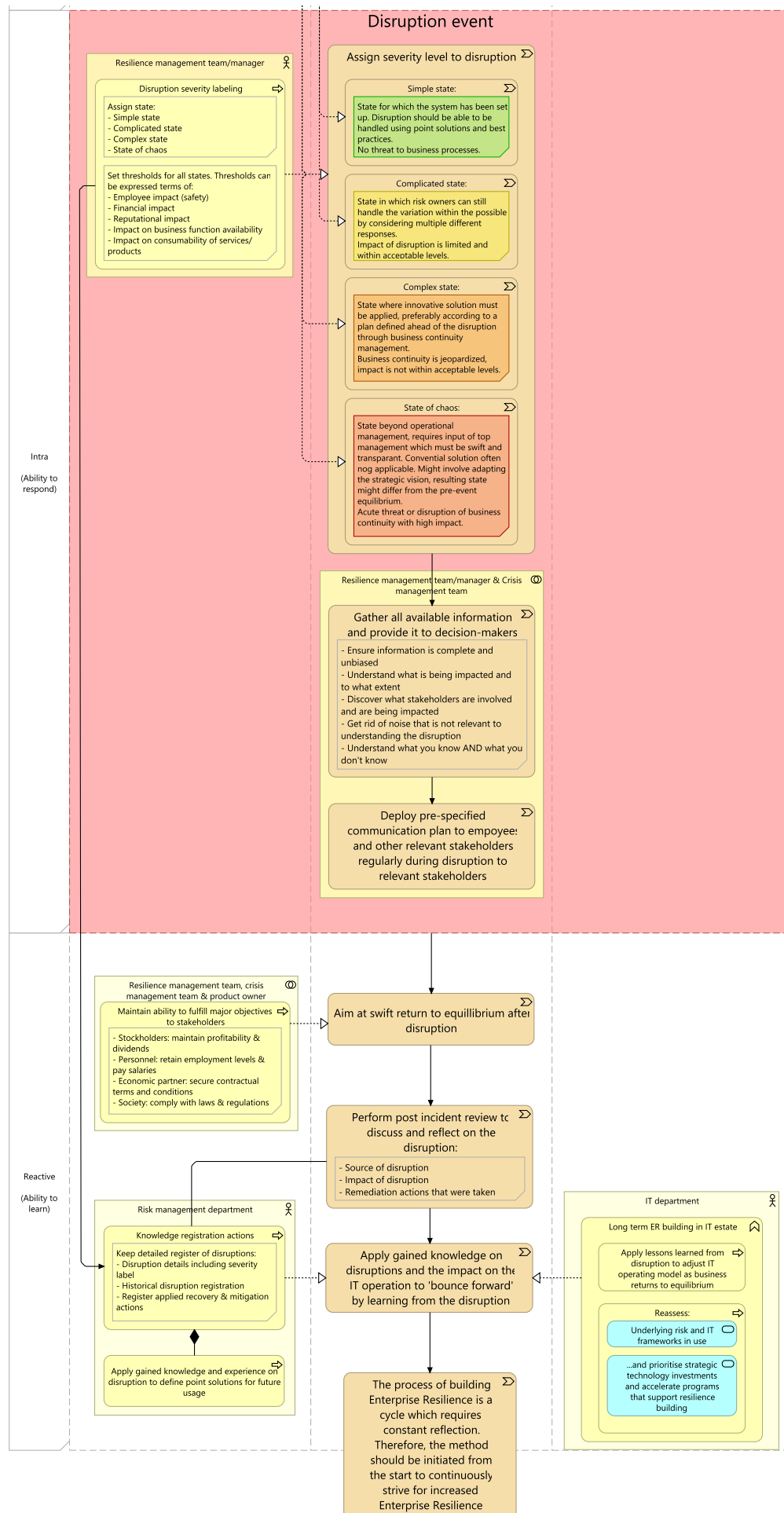
### ***Gather insights and lesson learned from the participant on method usage***

- Were the method and accompanying maturity model usable? How could it be improved?
- Were all activities and maturity levels clearly described?
- Was the design of the method clear to you in terms of dimensions? (proactive/intra/reactive & RM/aligned/ISM)
- Was the ArchiMate documentation sufficient to fully grasp the method?

# Appendix E: Method after treatment design cycle 2 (ER enhancement method, cycle 2)

[View full image online](#)






# Appendix F: Maturity Matrix continuous monitoring & auditing at Consulting firm















Bijlage III

## - Volwassenheidsmatrix

 Status heden (zomer 2022)

 Ambitie om op termijn te bereiken (2025)

In het controleplan hebben we aangegeven samen met Bedrijf X te willen groeien naar continuous monitoring en continuous auditing. Belangrijk hierbij is dat we gezamenlijk inzicht krijgen in wat uw huidige status is van continuous monitoring en uw ambitieniveau. Dit geldt ook ten aanzien van de verwachtingen van het accountantsproces. Onderstaand hebben wij onze inschatting weergegeven van onze eerste indrukken, graag bespreken we dit met u.

	1. Initial	2. Repeatable	3. Defined	4. Managed	5. Optimized
<b>People &amp; Governance</b>	No lines of defense in place and responsibility for risk management, internal controls and compliance are unclear	Coordination dependent on capabilities of individuals	Lines of defense defined, not fully integrated in the processes 	Capabilities are well defined and working towards lines of defense as integrated part of the business. Auditor can rely on evidence provided by client	Capabilities are well-defined and institutionalized, innovation-driven mindset 
<b>Process</b>	Minimum required internal control, processes are usually informal, incomplete and inconsistently applied	Processes defined but not documented and controls ad hoc and minimal verification 	Processes and controls defined, documented and understood 	Processes standardized and internal controls are embedded. Tooling is used to support this process (e.g. GRC)	Continuous Control Monitoring in place to continually improve internal controls and process efficiency 
<b>Technology &amp; Data</b>	IT is support, decentralized IT landscape, no standardization no emerging tech and absence of data infrastructure	IT fragmented, starting with harmonization and standardization of processes and IT 	IT is standardized, data warehouses available, starting with insights from data (e.g. KPI monitoring) 	Central data storage (e.g. datalake), mostly ad hoc insights, PoCs on emerging tech (e.g. Blockchain, AI)	Data intrinsic in decision making, central data lake, emerging tech fully embedded in processes 
<b>Compliance</b>	Focus on minimal requirements for compliance, no standard methodology in place, no systems to support compliance functions	Fragmented compliance, compliance controls in place not consistent across organization (limited to silos) 	Focus on standardized processes and compliance to main standards. Fragmented compliance systems are in place, but not central GRC platform 	Focus on compliance on multiple areas (e.g. social and governance). A central GRC system is used to support compliance processes	Focus on improvement of business processes & compliance to the standards on all areas 
<b>Communication</b>	Communication ad hoc and offline. Information is scattered across the organization	Information is scattered across the organization and communication mainly via e-mail 	Information is maintained centrally, and communication happens online (e.g. Skype) and e-mail 	Document management systems and collaboration tools are being used (e.g. Teams)	Fully digital, one platform is used for information sharing and communication 



# Appendix G: Maturity tracker (Excel)

[Download full sheet \(Google Drive\)](#)

[Mirror download \(Dropbox\)](#)

Enterprise Resilience enhancement method - Maturity tracker							
	Aligned ER building activities						
General Governance		Level	1	2	3	4	5
G.1	Reprioritize for resilience by reviewing planned changes and limiting non-critical changes to the IT estate to limit additional sources of disruption.	3	Changes are made without analysing the impact of the change in risk and the IT estate.		Change management is done with resilience in mind, an impact analysis is made for each major change.		Careful considerations are made before changes are made, the impact of every change on risk and IT is analysed. Non-critical changes are limited and are only made when resources are available to fully analyse the impact of the change. Overall, changes are not rushed and are efficiently implemented with resilience in mind.
G.2	A federated risk management approach is a balanced approach between departmental autonomy and common governance across departments regarding risk management. There is a common risk framework/approach, however, departments have the autonomy to determine how to execute it.	3	No common risk management framework/approach is implemented.		A risk management framework/approach is implemented and deployed enterprise-wide.		An effective risk management approach is implemented that gives departments the opportunity to adapt the common risk management approach/framework to their specific risk environment. Overall, each department has tuned the common risk management framework/approach.
G.3	Consider creating a cross-organizational resilience management team/position. Responsible for overseeing many of the resilience-building activities and promoting a culture that is open to learning from failure and aware of the importance of resilience.	3	No specific person or team is appointed to oversee building enterprise resilience.		An employee/employees are assigned to act as a resilience management team or position, depending on the size of the company. They are responsible for executing activities assigned to them in the Enterprise Resilience Enhancement method.		A dedicated cross-organizational resilience management team is created, responsible for activities assigned to them, as well as creating a company-wide resilience-aware culture. They have access to the resources needed to continuously build resilience.

G.4	Consider creating a crisis management team which is multifaceted and responsible for decision-making in case of a major disruption. It must consist of decision-makers, informers, and all parts of the business must be represented.	3	No crisis management team is appointed.	A crisis management team is appointed, decision-makers are part of the team.	A crisis management team is appointed and is made up of the required people. It consists of decision-makers (CEO, COO, CFO), representatives of all parts of the business (Legal, HR, facilities, etc.), and unbiased information providers (resilience manager, risk manager, business continuity manager). The team is prepared and knows their responsibilities in case of a disruption.
G.5	The usage of a centralized risk and resilience management tool offers an overview of the complete risk environment and is a central hub for overall analysis and reporting to support risk-intelligent decision-making.	3	No centralized risk and resilience management tool is implemented.	A centralized risk and resilience management tool is implemented and in use.	The centralized risk and resilience management tool is utilized to its maximum potential, it is integrated across the company and is actively used as a support tool for risk-intelligent decision-making.
Proactive					
P.1	Achieve full visibility of the enterprise and interweave with the identified risk environment.	3	The company is not actively monitoring any risk, they are unaware of potential disruption and how it can impact them. There also is no record of the business and IT infrastructure and is thus poorly fitted to the risk environment.	The company monitors their direct environment for disruptions and is aware of its business and IT infrastructure. This existing infrastructure is adequately adapted to the risks that the company faces in terms of redundancy.	The company has superior insights into their risk environment, they are fully aware of all known risks and their impact and are constantly monitoring for unknown risks. Also, complete visibility into the enterprise is achieved in terms of recording their business and IT infrastructure using enterprise architecture. The business and IT infrastructure are tuned to fit the risk environment, internal and third-party redundancy is implemented within this infrastructure.
P.2	Create a live feed that provides complete information from internal and external sources to increase awareness of your environment.	3	The company is not monitoring any internal and external sources for risk and is therefore mostly unaware of what is happening in their environment and in their company.	The company has access to crucial external information sources that report on possible disruption, like emergency services. Internally, possible sources of disruption are reported on, or monitored by the relevant decision-makers.	The company monitors as many external sources available as possible, from unbiased news outlets to extreme weather reports. A resilience manager/team will be notified as soon as a potential risk emerges, this feed of updates is monitored continuously. Internally they are fully aware of the status of all processes continuously, when disruption occurs all relevant decision-makers have access to the relevant information.

P.3	Establish a multimodal communication plan to inform stakeholders clearly and completely when a disruption occurs.	3	No pre-specified communication plan or mode of communication is available, it is also not known what stakeholders must be informed in case of disruption.	A communication plan is defined for the most important stakeholders. Enough information is supplied to these stakeholders to support decision-making.	A complete communication plan is available for all levels of disruption severity, it is known what stakeholders must be informed at what moment to support efficient and correct decision-making by the right people. A multimodal communication tool is available and can be quickly deployed, it increases the chance of notifying stakeholders early in case of disruption.
P.4	Proactive review of aspects that contribute to improved resilience. Involve ISM aspects in continuous risk and resilience monitoring.	3	The risk management process is undefined and not monitored. No attempts are made at building resilience using risk management or IT management frameworks.	A risk management process is implemented, this involves setting impact tolerances, risk identification, risk assessment, which are reviewed periodically.	There is a continuous review process on risk management process, risk tolerances are set, and the risk identification, assessment, and treatment processes are reviewed continuously, and when change occurs. Change is managed with resilience in mind, changes to business processes or the IT estate are reviewed to ensure a limited impact on the risk environment.
P.5	Regular testing of measures towards increasing Enterprise Resilience. The people that will be challenged must be involved with testing to build muscle memory. Crisis response plans, point solutions, business continuity plans, disaster recovery plans, and digital operational resilience must all be tested regularly.	3	Any measures in place to mitigate the chance of disruption are not tested. No effort is made to test how the company would be impacted in terms of resilience. The company is unsure about digital operational resilience and is susceptible to malicious attacks and outages.	Measures are tested periodically, the company has insights into the effectiveness of the tested measures and adjusts them accordingly.	All measures towards increasing Enterprise Resilience are tested continuously. The crisis response plan, point solutions for minor disruptions, business continuity plans, and disaster recovery plans are extensively tested with the involvement of the people that will be challenged when a real disruption occurs. The digital operational resilience is tested continuously by performing vulnerability assessments, network security assessments, gap analyses, performance testing, penetration testing, and performance testing. The company can ensure all measures are effective by adjusting them where needed.
Intra					
I.1	Severity level labelling during a disruption, and act accordingly.	3	The company does not label any disruptions and therefore has no way of acting according to the level of severity. This leads to wasted resources on minor disruptions or an inadequate reaction to major disruptions.	The company has implemented severity labels for disruptions. The relevant stakeholders are familiar with the labels and know how to act upon them.	The company has established a strict disruption labelling process that informs the relevant stakeholders immediately about their expected role. Thresholds are set that determine the level of severity, for each level it is known who is responsible for what.

I.2	Gather all available information and provide it to the relevant decision-makers. The information must be complete and unbiased. It described what is being impacted and to what extent, what stakeholders are involved, and describes what you know and what you don't know.	3	A very limited amount of information is collected and therefore decisions are made groundlessly when facing a disruption.	An effort is made to make sure the decision-makers are informed on the nature, impact, and severity of a disruption.	When a disruption occurs, all relevant information is collected at high speed by a dedicated actor. It is ensured that the information is unbiased, complete, and correct. This information is then timely communicated to the relevant decision-maker to put them in the optimal position to choose the correct steps forward.
I.3	Informing all employees and relevant stakeholders during a disruption, according to the pre-specified communication plan regularly.	3	No information on the nature of the disruption is shared with employees and other relevant stakeholders. Only the people directly involved with the disruption are aware of its existence.	All employees and stakeholders are informed in case of disruption according to a pre-specified communication plan.	All employees and relevant stakeholders are informed on a regular basis with the specific knowledge they need to bring them into a position to act or contribute in case this is needed. The process of informing all employees and relevant stakeholders is efficient and quick because it is done according to the pre-specified communication plan using a tool with multimodal communication capability.
Reactive					
R.1	The ability to swiftly return to equilibrium after a disruption using disaster recovery plans.	3	The company has to spend many resources over a long period of time to return to acceptable levels in terms of profitability, employment levels, and contractual obligations. Returning to pre-disruption levels is not a certainty. Partners, customers, or employees may be permanently lost.	The company is able to return to equilibrium at pre-disruption levels. This can be achieved by utilizing a reasonable amount of resources.	The company is able to apply disaster recovery plans and crisis remediation activities effectively, leading to successfully maintaining profitability, employment level, and contractual obligations. The company is able to swiftly and fully recover from these factors to pre-disruption levels. Minimal lasting damage is taken as a result of the disruption.
R.2	Perform post-incident review to discuss and reflect on the source, impact, and remediation actions to the disruption.	3	No post-incident review is performed.	A post-incident review is performed, during which the details in terms of source, impact, and remediation are discussed.	The company performs a complete post-incident review. This includes reflecting on the source, impact, and remediation action of the disruption. Stakeholders that may have been at the source of the disruption are involved in this, as well as the stakeholders that responded to the disruption. Depending on the severity of the disruption, a full report may be made and reflected on. The goal of the post-incident review is to define new or adjusted mitigation actions for the disruption.

R.3	Apply gained knowledge on disruptions and their impact on the IT operation to 'bounce forward' by learning from the disruption. This knowledge must be used to better prepare for similar disruptions in the future.	3	No knowledge registration actions are performed, the company makes no effort to learn from the disruption.	Knowledge registration actions are performed, the details from the post-incident review are recorded and can fall back on it in case a similar disruption occurs in the future.	Once the company has recovered from the disruption, it is seen as a learning opportunity. The company reflects on the remediation actions and learns from them by applying what was learned to the improvement of point solutions, business continuity plans, disaster recovery plans, and crisis response plans.
R.4	The process of building Enterprise Resilience is a cycle which requires constant reflection. Therefore, the method should be initiated from the start to continuously strive for increased Enterprise Resilience.	3	When the disruption has been handled and the company returns to equilibrium, no more actions are performed relating to building Enterprise Resilience.	The company reflects on the disruption and applies lessons learned from the disruption. They continue anticipating and monitoring according to the proactive activities (P.1-P.5).	When the disruption has been resolved, the company actively continues to improve Enterprise Resilience. They reflect on their operating model in relation to risk and IT, this may involve adapting the underlying risk frameworks and IT management frameworks. They continue anticipating and monitoring according to the proactive activities (P.1-P.5).
<b>Total:</b> (Min: 17 - Max: 85)		<b>51</b>	50,00%		
General governance total (max 25)		15	50,0%		
Proactive total (max 25)		15	50,0%		
Intra total (max 15)		9	50,0%		
Reactive total (20 total)		12	50,0%		

## Appendix H: Case study 1, maturity tracker results (Participant 3.1)

Aligned ER building activities		
General Governance		Level
G.1	Reprioritize for resilience by reviewing planned changes and limiting non-critical changes to the IT estate to limit additional sources of disruption.	1
G.2	A federated risk management approach is a balanced approach between departmental autonomy and common governance across departments regarding risk management. There is a common risk framework/approach, however, departments have the autonomy to determine how to execute it.	3
G.3	Consider creating a cross-organizational resilience management team/position. Responsible for overseeing many of the resilience-building activities and promoting a culture that is open to learning from failure and aware of the importance of resilience.	2
G.4	Consider creating a crisis management team which is multifaceted and responsible for decision-making in case of a major disruption. It must consist of decision-makers, informers, and all parts of the business must be represented.	2
G.5	The usage of a centralized risk and resilience management tool offers an overview of the complete risk environment and is a central hub for overall analysis and reporting to support risk-intelligent decision-making.	3
Proactive		
P.1	Achieve full visibility of the enterprise and interweave with the identified risk environment.	2
P.2	Create a live feed that provides complete information from internal and external sources to increase awareness of your environment.	3
P.3	Establish a multimodal communication plan to inform stakeholders clearly and completely when a disruption occurs.	5
P.4	Proactive review of aspects that contribute to improved resilience. Involve ISM aspects in continuous risk and resilience monitoring.	1
P.5	Regular testing of measures towards increasing Enterprise Resilience. The people that will be challenged must be involved with testing to build muscle memory. Crisis response plans, point solutions, business continuity plans, disaster recovery plans, and digital operational resilience must all be tested regularly.	3
Intra		
I.1	Severity level labelling during a disruption, and act accordingly.	5
I.2	Gather all available information and provide it to the relevant decision-makers. The information must be complete and unbiased. It described what is being impacted and to what extent, what stakeholders are involved, and describes what you know and what you don't know.	4

I.3	Informing all employees and relevant stakeholders during a disruption, according to the pre-specified communication plan regularly.	2
<b>Reactive</b>		
R.1	The ability to swiftly return to equilibrium after a disruption using disaster recovery plans.	2
R.2	Perform post-incident review to discuss and reflect on the source, impact, and remediation actions to the disruption.	4
R.3	Apply gained knowledge on disruptions and their impact on the IT operation to 'bounce forward' by learning from the disruption. This knowledge must be used to better prepare for similar disruptions in the future.	2
R.4	The process of building Enterprise Resilience is a cycle which requires constant reflection. Therefore, the method should be initiated from the start to continuously strive for increased Enterprise Resilience.	3

<b>Total:</b> (Min: 17 - Max: 85)	<b>47</b>	<b>44,12%</b>
--------------------------------------	-----------	---------------

<b>General governance total (max 25)</b>	11	<b>30,0%</b>
<b>Proactive total (max 25)</b>	14	<b>45,0%</b>
<b>Intra total (max 15)</b>	11	<b>66,7%</b>
<b>Reactive total (max 20)</b>	11	<b>43,8%</b>

## Appendix I: Case study 2, maturity tracker results (Participant 3.2)

Aligned ER building activities		
General Governance		Level
G.1	Reprioritize for resilience by reviewing planned changes and limiting non-critical changes to the IT estate to limit additional sources of disruption.	3
G.2	A federated risk management approach is a balanced approach between departmental autonomy and common governance across departments regarding risk management. There is a common risk framework/approach, however, departments have the autonomy to determine how to execute it.	3
G.3	Consider creating a cross-organizational resilience management team/position. Responsible for overseeing many of the resilience-building activities and promoting a culture that is open to learning from failure and aware of the importance of resilience.	4
G.4	Consider creating a crisis management team which is multifaceted and responsible for decision-making in case of a major disruption. It must consist of decision-makers, informers, and all parts of the business must be represented.	3
G.5	The usage of a centralized risk and resilience management tool offers an overview of the complete risk environment and is a central hub for overall analysis and reporting to support risk-intelligent decision-making.	2
Proactive		
P.1	Achieve full visibility of the enterprise and interweave with the identified risk environment.	3
P.2	Create a live feed that provides complete information from internal and external sources to increase awareness of your environment.	3
P.3	Establish a multimodal communication plan to inform stakeholders clearly and completely when a disruption occurs.	2
P.4	Proactive review of aspects that contribute to improved resilience. Involve ISM aspects in continuous risk and resilience monitoring.	2
P.5	Regular testing of measures towards increasing Enterprise Resilience. The people that will be challenged must be involved with testing to build muscle memory. Crisis response plans, point solutions, business continuity plans, disaster recovery plans, and digital operational resilience must all be tested regularly.	2
Intra		
I.1	Severity level labelling during a disruption, and act accordingly.	2
I.2	Gather all available information and provide it to the relevant decision-makers. The information must be complete and unbiased. It described what is being impacted and to what extent, what stakeholders are involved, and describes what you know and what you don't know.	4



I.3	Informing all employees and relevant stakeholders during a disruption, according to the pre-specified communication plan regularly.	2
<b>Reactive</b>		
R.1	The ability to swiftly return to equilibrium after a disruption using disaster recovery plans.	3
R.2	Perform post-incident review to discuss and reflect on the source, impact, and remediation actions to the disruption.	3
R.3	Apply gained knowledge on disruptions and their impact on the IT operation to 'bounce forward' by learning from the disruption. This knowledge must be used to better prepare for similar disruptions in the future.	2
R.4	The process of building Enterprise Resilience is a cycle which requires constant reflection. Therefore, the method should be initiated from the start to continuously strive for increased Enterprise Resilience.	3

<b>Total:</b> (Min: 17 - Max: 85)	<b>46</b>	<b>42,65%</b>
--------------------------------------	-----------	---------------

<b>General governance total (max 25)</b>	15	<b>50,0%</b>
<b>Proactive total (max 25)</b>	12	<b>35,0%</b>
<b>Intra total (max 15)</b>	8	<b>41,7%</b>
<b>Reactive total (20 total)</b>	11	<b>43,8%</b>