Spring 3-2022

# Aligning Recovery Objectives With Organizational Capabilities

Jude C. Ejiobi
*Dakota State University*

# ALIGNING RECOVERY OBJECTIVES WITH ORGANIZATIONAL CAPABILITIES

A dissertation submitted to Dakota State University in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Cyber Operations

March 2022

By

Jude C. Ejiobi

Dissertation Committee:

Shengjie Xu Ph.D.
Omar El-Gayar Ph.D.
Austin O'Brien Ph.D.

DAKOTA STATE UNIVERSITY

# DISSERTATION APPROVAL FORM

This dissertation is approved as a credible and independent investigation by a candidate for the Doctor of Philosophy degree and is acceptable for meeting the dissertation requirements for this degree. Acceptance of this dissertation does not imply that the conclusions reached by the candidate are necessarily the conclusions of the major department or university.

Student Name: Jude C. Ejiobi

Dissertation Title: Aligning Recovery Objectives with Organizational Capabilities

Dissertation Chair/Co-Chair: Shengjie Xu Date: April 15, 2022

Name: Shengjie Xu

Dissertation Chair/Co-Chair: __________ Date: __________

Name:

Committee member: Omar El-Gayar Date: April 15, 2022

Name: Omar El-Gayar

Committee member: __________ Date: April 15, 2022

Name: Austin O'Brien

Committee member: __________ Date: __________

Name:

Committee member: __________ Date: __________

Name:

Original to Office of Graduate Studies and Research
Acid-free copies with written reports to library

# ACKNOWLEDGMENT

I am grateful to everyone who has contributed to this research directly or indirectly. From those from whom I have drawn inspiration, to those who assisted and encouraged me throughout this journey. I hope that the results can inspire others in their undertaking just like I have been inspired.

My sincerest gratitude is to my dissertation committee members, Dr. Omar El-Gayar, Dr. Austin O'Brien, and chaired by Dr. Shengjie Xu, for their support, encouragement, patience, and understanding, especially in very challenging circumstances. I also acknowledge the support and encouragement of my adviser Dr. Yong Wang as well as the very knowledgeable and capable faculty at the School of Computer and Cyber Sciences at Dakota State University.

I cannot help but feel like the conclusion of this program has given me a new life purpose. I am hopeful that this is the case. As I continue to see what the future holds, I am glad to say that even though it has been very challenging, it has also been rewarding.

To the practitioners who participated in the study, your contributions will hopefully benefit the discipline and practice on a broader scale. For that I am grateful!

To my parents, Nze and Lolo Ejiobi both of blessed memory, I know that you would be proud. Your unconditional love has always been my greatest inspiration.

At the beginning of this research, I wanted to learn how something is done. In the process, I gained more clarity on why it should be done in the first place. This perhaps confirms the thoughts of Fredrick Niechze, "He who has a "why" to live for can almost bear any "how"."

# ABSTRACT

To reduce or eliminate the impact of a cyber-attack on an organization, preparations to recover a failed system and/or data are usually made in anticipation of such an attack. To avoid a false sense of security, these preparations should, as closely as possible, reflect the organization's capabilities, in order to inform future improvement and avoid unattainable goals. There is an absence of a strong basis for the selection of the metrics that are used to measure preparation. Informal and unreliable processes are widely used, and they often result in metrics that conflict with the organization's capabilities and interests. The goal of this research was to establish a process that could be used to assess and validate an organization's recovery objectives by ensuring the selection of metrics that align with the organization's true capabilities.

To form the basis for a formalized process for selecting recovery metrics, a decision model is proposed to ensure that, at the minimum, an organization's technical capabilities are considered, and that on the other hand, risk tolerance thresholds are not exceeded. A short survey of qualified practitioners was conducted to determine the preferred recovery metrics and other important priorities based on the expected impact of a cyber-attack. The results revealed that organizations mostly prefer to use the popular or well-known recovery objectives (RTO and RPO), and it was demonstrated that by using a clear and well-defined process, these metrics can be objectively and reliably established. Finally, considering the capabilities of an organization's information systems, mathematical relationships between these metrics and other existing recovery metrics are proposed as part of the decision model to ensure that these recovery objectives are established within the organization's technical and economic limits.

The resulting artifact was first evaluated using a numeric experiment to demonstrate its mathematical and technical soundness. It was then compared directly to previously proposed models using five different criteria to validate its ability to contribute meaningfully to the solution sought for the research problem. The comparison confirmed the utility, feasibility, repeatability, and reliability of the proposed solution. The artifact was then applied in a case study using an illustrative scenario comprising of real-world statistics. The findings were used to demonstrate that if a history of an information system's performance in preparatory activities such as backup operations and recovery drills is incorporated into decisions concerning the selection of recovery objectives, the resulting metrics will more accurately represent the ability to satisfactorily recover the systems in an actual incident. This was verified by recommendations based on established frameworks. Finally, the resulting model was presented to qualified experts for expert opinion, and positive feedback was received from both technical and business operations perspectives. It was then concluded that recovery objectives can be established in alignment with the relevant details of an organization's information systems, and that the impact on the organization's ability to conduct recovery operations more effectively will be positive.

# DECLARATION

I hereby certify that this dissertation constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions, or writings of another.

I declare that the dissertation describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,

Jude Ejiobi

Jude C. Ejiobi

# TABLE OF CONTENTS

# LIST OF TABLES

# LIST OF FIGURES

# CHAPTER 1
# INTRODUCTION

Traditionally, most organizations have addressed the threats posed by both natural and man-made disasters by establishing recovery objectives. These are thresholds by which they assess their readiness to recover from an incident and return to normal operation. Of the several recovery objectives that have been proposed, the two most important and most popularly used are the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO) (Thomas, Gordon, & Galligher, 2018). The RTO establishes the timeframe within which the organization expects to recover the failed system to full functionality. On the other hand, the RPO usually refers to the tolerable data loss expectancy (Thomas et al., 2018). Both metrics have been used extensively and quite successfully to establish an organization's position on the preparedness scale, as well as its ability to recover from a severe cyber incident. In the context of organizational cybersecurity strategy and since recovery for cyber incidents and natural disasters are planned to use similar architectures (Sicard, 2019), many organizations use the same metrics to assess their readiness for cyber incidents by targeting both the amount of data that can be recovered and the timeliness of that recovery. However, how these metrics are established for non-adversarial incidents may not necessarily be applicable for cyber incidents, especially intentional or adversarial attacks.

## 1.1. Background of the Problem

As the threats posed by cyber-attacks to organizations increase in sophistication and volume, organizations are compelled to take a preemptive approach in understanding these threats in order to defeat them. This has in many cases moved “preparedness” closer to the top of the cybersecurity agenda (Gomes, Ahokangas, & Owusu, 2016). As part of the preparation for cyber incident recovery, organizations need to test both their ability to recover their critical systems and their ability to initiate and successfully execute the steps in the recovery process. The results of these tests, in the absence of an actual incident, can be used to demonstrate preparedness or lack thereof. This is usually done to satisfy or justify the dedication of resources to incident recovery in such areas as budgeting and regulatory compliance (Podofillini, Wolfgang, Bruno & Bozidar, 2015). To use these results for the said purposes, the performance of the system during a test or assessment is captured and recorded.

Experience and research in both industry and academia have shown that Recovery Objectives are established by organizations using subjective and informal methods, either to satisfy regulatory requirements or merely to demonstrate conformance to good practice (Bodeau, Graubart, McQuaid, & Woodill, 2018).

## 1.2. Research Motivation

Several studies, as will be seen later in this section, have shown that when recovery planning is poor, most organizations are unable to recover from a successful and severe cyber incident, and in some cases, the consequences are extreme for these organizations. About 60% of businesses will fail within 6 months of a severe cyber-attack (Koulopoulos, 2017), and 50% of organizations without a recovery plan will never reopen for business after a major incident (Rabbani, Soufi, & Torabi, 2016). Steinberg (2019) cited a study done by Accenture in 2019 which noted that 43% of all cyber-attacks were aimed at small businesses and that only 14% of them were prepared to defend themselves. The article also noted cybercrime as the “fastest-growing form of criminal activity” (Steinberg, 2019). These numbers demonstrate the urgent need for the reliability of adequate preparation in organizational cyber incident recovery. In addition, there is an absence of legislative or regulatory requirement for organizations to recover failed systems within a certain timeframe, leaving organizations to set their own recovery standards.

A major corner piece of these standards is the set of recovery objectives used by organizations to assess readiness for cyber incidents. The most widely used of these objectives are the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO). A recent study by Goodwin (2021) noted that the average time between backups is 24 hours while the most common RPO and RTO are 1 – 4 hours and 4 – 8 hours respectively. Another study by Veritas (2020) revealed that 66% of organizations estimated more than a five-day recovery time from incidents such as ransomware if the ransom is not paid. This demonstrates a mismatch between the recovery objectives being selected and the organizations' recovery capabilities.

In system recovery operations, the reliability of both the backup data and the process in which it is used depends greatly on how the backup is collected in the first place. This suggests that aside from quality and integrity, the timing, with regards to the collection and use of backup data, is an essential factor. Both the RTO and RPO are references to several points in time, and proper alignment of these points in time with the overall process can improve the final outcome of data and system recovery.

## 1.3. Research Problem

Organizations periodically test their capabilities in systems recovery by assessing their technical and administrative resources. This is usually done for several reasons that include regulatory requirements, internal cybersecurity hygiene, and stakeholder assurance. To demonstrate or test preparedness for recovery, certain thresholds are established and used as a yardstick to evaluate recovery capabilities. It is generally in the organization’s best interest to keep the RTO and RPO low (Alhazmi, 2015), and since reducing these numbers increases the cost of recovery planning (Alhazmi, 2015), the dynamics between business interests and IT interests are almost always in conflict. Regardless of the reason why an organization conducts these assessments, a clear method for setting these objectives does not exist in either academic or industry lexicon. Onwubiko (2020) also noted that research dedicated to cyber incident recovery are unfortunately lacking.

Recovery metrics have traditionally been limited, either to an organization’s technical capabilities or to mere suggestions by its business operations of the threshold of tolerable impact. This seldom reflects an organization’s actual tolerance or risk appetite. Recovery metrics that do not reflect an organization’s true capabilities, when used as a basis for testing for preparedness, can provide a false sense of security for the organization and result in a failure to recover the failed systems within reasonable parameters in the event of an actual cyber incident. For this reason, the parameters that define the relationship among the recovery metrics should be well defined so that when establishing these metrics, the limits are understood, and unnecessary overlaps are avoided.

### 1.3.1. Issues with Recovery Time

If a clear distinction between the Maximum Tolerable Downtime (MTD) and Recovery Time Objective (RTO) is not made, these two terms tend to be used interchangeably, and this can present problems in the long run (NIST, 2021). One way to distinguish between the two is to establish a mathematical relationship between both terms. Taken quite literally, and according to many standard definitions, the MTD is the total amount of time an organization is willing to accept for an outage or disruption during which it must recover its systems and data to avoid an intolerable impact to the organization (NIST, 2021). This means that the RTO, also if taken literally, should be an objective or goal set by the organization to test its ability to recover its systems and/or data within the timeframe established by the MTD (Kawaguchi, 2013). If this is the case, then as noted by NIST (2021) the relationship between the MTD and RTO can be expressed as follows:

$$MTD \geq RTO \tag{1}$$

While this seems mathematically feasible it presents a problem which is that, at some point, the MTD could be equal to the RTO. This also means that if the RTO is exceeded or if recovery is not successfully completed within this timeframe, the organization would already be experiencing an intolerable impact from the incident. For this reason, it is important to establish the RTO in a way that accounts for the restoration of the organization's critical IT infrastructure sub-systems and still leave a sufficient time "cushion" between it and the MTD (Kawaguchi, 2013).

### 1.3.2. Issues with Recovery Point

An organization has to determine how much data it is capable of recovering and how much it is willing to lose following a disruptive incident (NIST, 2021). Because all organizations process and store different amounts of data, this value is usually expressed as a reference to a point in time rather than as a quantity of data, using the Recovery Point Objective (RPO) metric (Chow, Deshpande, Seshadri & Liu, 2021). Recovery of systems and data is usually done using Backups which are essentially a detailed record of the status of the organization's systems and data at a point in time. This record is taken in a particular cadence that is usually a reflection of the organization's commitment to "Availability." More frequent backups usually require a higher investment in the technologies and other resources that make them possible (Goodwin, 2021).

To minimize data loss following a disruptive incident, information systems should be restored using the most recent backup data (NIST, 2021). This, if done successfully, restores the system to the most recent point in time that the last valid backup was taken. This also establishes the technical limitation of an organization's recovery systems and makes it impossible to achieve an RPO that does not mathematically agree with the Backup Frequency. In other words, the relationship between the RPO and the Backup Frequency represented as $F$ in equation 2 is that RPO must be larger or equal to $F$. This relationship can be expressed as follows:

$$F \leq RPO \tag{2}$$

Similar to the issues with the RTO and MTD relationship, the Backup frequency $F$ can equal RPO at some point. This means that the inability to successfully restore data from a backup due to a reason such as the failure or corruption of backup data can make it uncertain that the recovery point objective will be achieved (Goodwin, 2021).

### 1.3.3. Problem Statement

Since organizations have the prerogative responsibility to select their own recovery objectives, without a clearly defined process there is no way to assure that these selections are not in conflict with the organization's limits with regards to tolerance for outage and recovery capabilities. A recent study completed by Goodwin (2021) revealed that, on average, backups are taken at intervals of 24 hours, while the average RPO is 1 – 4 hours.

Other metrics involved in system recovery such as MTD and Backup Frequency are objectively obtainable from business processes, but their relationships with the standard and generally accepted recovery objectives have largely remained undefined. As a result, the process for selecting recovery objectives is usually subjective, varied, and mostly informal. The potential consequences of this have created a gap in incident response and recovery that researchers have attempted but have not been able to close. One of such consequences is that recovery objectives, being the responsibility of the organizations, due to a lack of a formalized process, are not logically defensible. Also, from the perspective of accountability and due diligence, they are difficult to justify. A review of the previous work done in the attempts to address this problem is presented in Chapter 2.

### 1.3.4. Research Question

The inconsistencies that exist in the relationship among these recovery metrics present a problem in how the metrics are derived and established. This has led to the following research question:

> *How can Recovery Time and Data Loss Expectancy metrics be established so that they truly reflect an organization's ability to recover its systems from a cyber incident within tolerable limits?*

This research answers this question by proposing a decision model for deriving logically applicable and defensible recovery objectives or metrics that demonstrate an organization's true capabilities and recognizes its tolerance limits.

## 1.4. Research Objective

The objective of this research is to address the research problem by identifying what organizational concerns and interests are, regarding the selection of recovery objectives, and to offer a feasible solution based on this understanding that is aimed at closing the research gap.

Specifically, the intended contribution would be a decision model to standardize the process of establishing the well-known and preferred recovery metrics (RTO and RPO) in a manner that is objective and feasible. It is also expected that recovery objectives established using this model will be more dependable as they will be verifiable, defensible, and respectful of the organization's technical and economic limits.

## 1.5. Assumptions

To aid the efforts in this research and support the creation and validation of the decision model, the following assumptions were made:

- A Business Impact Analysis is performed, and the results demonstrate the organization's maximum tolerance for system outage
- Information systems are organized in a logical hierarchy, and therefore recovered according to the layout of sub-systems in the order of this hierarchy, as shown in Table 1
- A recovery operation, specifically with regards to testing, will involve all layers or subsystems in the IT environment
- For components outside the organization's control, the reliability of networks as defined by Xu, Qian, and Hu (2018), and other supporting and auxiliary resources are assured
- There is a degree of dependency between a subsystem and that which precedes it in the hierarchy of the IT architecture
- Full functionality of a subsystem requires all functionality of all hierarchically preceding subsystems.

In Table 1, the subsystems of a typical IT infrastructure are shown in the hierarchical order of operation [and therefore recovery] starting from the bottom. This hierarchy is based partly on the technical dependencies as expressed in the OSI and TCP/IP reference models but was modeled after existing recovery management levels shown in Fig. 1 and Fig. 2, based on technical dependencies.

Table 1. Recovery Hierarchy Stack

| Tier | Infrastructure Layers (Sub-system) |
|---|---|
| 5 | Application |
| 4 | Database |
| 3 | Network |
| 2 | Compute |
| 1 | Storage |

Fig. 1 is a representation of the logical order in which recovery technologies are organized in a virtualized environment. The "Recovery Hierarchy Stack" presented in Table 1 is an adjustment of the components of the "Virtualization" layer and the "Volume Management" layer to reflect a basic organization's IT infrastructure and reflect the recovery process for disruptions specific to cyber incidents. Also, Table 1 refers to the "services" of each of the layers within the organization's IT environment and does not include components or resources that may not be readily available for recovery operations. Fig. 2 is also an example of the application of a layered recovery technology process to disaster recovery.

Regardless of the exact configuration used, it is evident that the layers represented are similar. It is also important to note that the "Network" layer referenced in the Recovery

Hierarchy Stack is the internal network, and is separate from, and along with all the other tiers, dependent on the reliability of external network infrastructure as defined by Xu et al (2017).

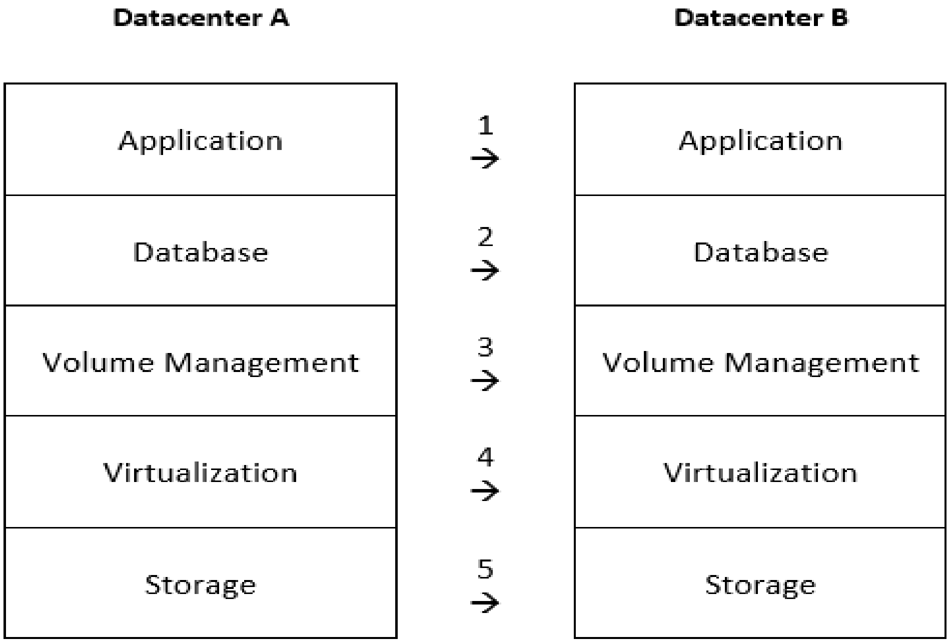
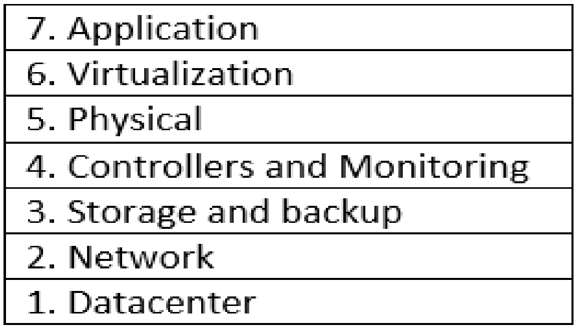


Figure 1. Levels of Disaster Recovery Technology (Zhu et al., 2017)



| |
|---|
| 7. Application |
| 6. Virtualization |
| 5. Physical |
| 4. Controllers and Monitoring |
| 3. Storage and backup |
| 2. Network |
| 1. Datacenter |

Figure 2. DR Layers (Baham et al., 2017)

## 1.6. Paper Outline

In Chapter 1, details of the research problem were discussed. These included a description and relevance of the popular recovery objectives, the research question addressed, and assumptions made. The remainder of this paper is organized as follows: In Chapter 2, the related work of several authors and researchers who have attempted to objectify the selection and use of recovery metrics are presented. Chapter 3 discusses the items required to craft a solution to the research problem as defined by practitioners and prior postulations. In Chapter 4, the research methodology used is presented, discussed, and justified. The artifact or decision model is presented and discussed in Chapter 5, and its components and potential performance are examined and evaluated in Chapter 6.  The results of the evaluation are presented in Chapter 7, and the conclusion of the research along with suggested future research work are discussed in the final chapter.

# CHAPTER 2
# LITERATURE REVIEW

## 2.1. Introduction

Cyber threats and incidents continue to emerge and have evolved over time, and this has caused scholars and researchers in both academia and industry to pursue several ways to establish the most widely used assessment metrics (RTO and RPO). Some researchers have proposed the use of the Analytical Hierarchy Process but have mostly been focused on the development of Information Security policies. Other proposals have been offered, some of which feature several models and their attempted use to derive the popular metrics (RTO and RPO), while others offer a completely different set of metrics.

## 2.2. Multi-criteria Decision Making

Authors, researchers, and practitioners, as discussed in the next paragraph, have used the Analytical Hierarchy Process to facilitate and improve decision-making processes in information security. However, these efforts have targeted either the development of information security policies or the selection of information security controls. None so far have been geared towards the factors that affect the objectivity of the metrics that guide the recovery of systems with regards to time and data.

Using the Analytical Hierarchy Process, Gedam and Meshram (2019) sought to prioritize security requirements in Object-Oriented Software Development. Cabrera, Luceno Reyes, and Lasco (2021) also attempted to improve decision-making processes by employing the Analytical Hierarchy Process. They used security goals (the CIA triad) as the alternatives and the four aspects of information security (technology, management, economy, and culture) as criteria. Tariq et al. (2020) recognized the importance of prioritizing information security decisions around some criteria, especially with the advent of wireless sensor networks and cloud computing and proposed the "Fuzzy AHP." In a case study on the Evaluation of Disaster Recovery (DR) strategies, Mendonca, Lima, Andrade, Araujo, and Kim (2020) adopted Little's Law by dividing the number of requests by the arrival rate to obtain the Mean Response Time to compute RTO and RPO. None of the aforementioned attempts address an organization's ability to recover its systems and data within tolerable limits.

## 2.3. Other Metrics

In the context of organizational cybersecurity, and because the impact of cyber incidents, like those of natural disasters, are both hard to predict, and impact the organization in ways similar to natural disasters (Carias et al., 2019), many organizations prefer to use the same metrics as those used for natural disasters to assess their readiness for cyber incidents. This means that they consider both the ability to recover data and the timeliness of a recovery operation. Recently, different schools of thought have emerged, suggesting that the nature of cyber incidents differs enough from traditional disasters to justify a different approach in assessing recovery performance (Podofillini et al., 2015). The reason often given is that cyber-attacks, in general, differ in their methods of operation, therefore it can be difficult to accurately establish the exact time, scale, and even impact of an attack.

Bodeau, Graubart, McQuaid, and Woodill (2018) defined cyber resilience as a combination of three different metrics which are, Security Metrics, Resilience Metrics, and Risk Metrics. They state that any single metric should be treated as the starting point of a discussion, as all metrics might mean different things to different stakeholders. Bodeau et al. (2018) also acknowledged some challenges regarding complexity, contextuality, and feasibility. They offer these as their reasons for pursuing a more comprehensive view of resilience rather than just the recovery of systems and data. They argued that goals such as anticipation, adaptation, prevention, reconstitution, and damage limitation belong in the context of cyber resilience and recovery. The authors offer alternative metrics to the traditional recovery metrics as more appropriate. Two of the more prominent of these are, Measure of Effectiveness (MoE) and Measure of Performance (MoP). Overall, the approach the authors advocated for seems very robust and complex. As many as 47 different metrics were identified and the advocacy for a single figure metric was acknowledged. Finally, the fact that many organizations don't necessarily base engineering and budgeting decisions on these metrics was pointed out in this publication. Bodeau et al. (2018) also stated that many organizations simply establish metrics to demonstrate compliance or conformance to good practices.

Podofillini et al., (2015) describes the traditional methods of using backups for recovery as appropriate for physical risks and claimed that they usually fail in the case of cyber disasters. They acknowledged that recovery procedures and metrics that address cyber incidents specifically are in their early stages, but that returning to normal operation within specific times, even if the cyber incident has not been fully resolved, can be crucial depending on the type of organization and its overall mission. They used the Sony Entertainment cyber incident as evidence that RTO and RPO are not feasible because, after the attack on Sony, several computers stayed inaccessible for several days regardless of what their established recovery objectives were. Podofillini et al., (2015) acknowledged metrics such as the Non-Disclosure Objective (NDO) and the Recovery Consistency Objective (RCO) as more appropriate metrics for measuring the ability of an organization to recover from a cyber incident and return to normal business operation. They also pointed out the multiple-stage nature of some cyber-attacks and claimed that the exact time of compromise can be difficult to determine. Finally, Podofillini et al., (2015) noted that there is no generally accepted resilience level for every industry. They suggested that recovery planning should be tailored to specific organizational needs, but also noted that they expect that in the future, regulatory authorities will impose recovery obligations on different industries.

Arul et al., (2017) noted that cyber-attacks happen when information or systems are exposed and exploited. In their article for the Cloud Security Alliance, the authors recognized that sometimes the time of discovery is not the same as the time of occurrence. With that, they proposed a new set of metrics to identify and track this lapse in time. These are, Elapsed Time to Identify Threat (ETIT) and Elapsed Time to Identify Failure (ETIF). This is further acknowledgment that cyber incidents are organic in nature and can best be objectified by a strong alignment with the objectives of the organization.

### 2.3.1. Summary of Other Metrics

The metrics suggested by previous researchers all reference one important factor in system recovery which is “time.” This is because the impact of a cyber incident on an organization, when the adversarial intent is to disrupt system and data availability, can be referenced to time. The cost of the downtime caused by the incident and the loss of valuable data based on the amount of recoverable data appear to be consistent goals of all the offerings made so far.

## 2.4. Previous Models and Solutions for RTO and RPO

Research efforts in the past have produced processes or models that were intended to address the stated research problem. However, these efforts have in one way or the other, fallen short of providing a reliable set of metrics that are logically defensible, especially in the context of this research.

### 2.4.1. Gap Time Reduction

Kawaguchi (2013) offered a “Twin Model” which features a combined “RTO Model” and “Current Recovery Time (CRT) Model” to achieve a “Gap Time Reduction” which is the reduction of the time between the CRT and the MTD. The authors present that understanding the desired gap between the MTD [which was represented as the Maximum Tolerable Period of Disruption (MTPD)] and the CRT, prior to setting the RTO, is essential. This approach does not consider the gap between the MTD and the RTO, as exceeding the RTO by an uncontrolled margin puts the organization’s recovery time either dangerously within “striking distance” of the MTD, or even above it. Finally, although Kawaguchi (2013) differentiates between the currently stated recovery capabilities and the recovery goal with regards to the time of recovery, the model proposed only utilizes the organization’s budget rather than a history of its past performances.

### 2.4.2. Multi-Objective Scenario-Based Stochastic Robust Optimization

A Multi-Objective Scenario-Based Stochastic Robust Optimization model proposed by Sahebjamnia, Torabi, Mansouri, and Salehi (2011) was aimed at uncertainties introduced by the likelihood and impact of a disaster. The researchers attempted to generate efficient recovery solutions by maximizing the value of recovery capability and completeness, and minimizing the cost of recovery (Sahebjamnia, Torabi, Mansouri & Salehi, 2011). In this model, the types of disasters planned for are primarily natural, therefore the likelihood and impact variables considered only apply to natural disasters. This implies that the resulting risk calculations do not include the characteristics of a typical cyber incident and are therefore unreliable in the context of this research. Also, the product of the model is a single objective scenario, the Recovery Time, along with its relative associated cost. A relationship with the maximum tolerable limit is not expressed and neither are the recovery point and acceptable data loss parameters.

### 2.4.3. Smart Recovery Advisor

Aimed at fostering Continuous Data Protection (CDP), Chow, Deshpande, Seshadri & Liu (2021) offered the Smart Recovery Advisor (SRA) which focuses on optimizing the selection of a recovery point. The primary objective and capability of the SRA are to detect and recommend valid restore points to which recovery operations can be targeted. Focusing on the recovery point and data loss, this model features a feedback system that uses a "learning" process based on the performance and history of the backup and restore operations. The SRA however does not have any features that take into consideration the organization's socio-economic priorities. It also does not address recovery times as well as the organization's tolerance in periods of disruption.

### 2.4.4. Computer-Aided Disaster Recovery Planning Tools

As system recovery depends mainly on the availability of alternate data, data and systems need to be backed up to ensure this availability (Alhazmi, 2015). Alhazmi (2015) acknowledged that a knowledge of the organization's priorities is necessary for adequate recovery planning. Based on this, and IBM's 7 tier system for disaster recovery planning (DRP), Alhazmi (2015) proposed a software tool that enhances disaster recovery planning by simulating IT DRP systems. This system neither informs the creation of recovery objectives in a way that accounts for prior system performance nor factors the organization's tolerance for disruptive incidents. It only compares the selection of different DRP solutions based on available technology and their associated costs.

### 2.4.5. Contingency Planning in Digital Recording Company

In a study done on a music and digital recording company, Ruddin, Santoso, Indrajit, and Dazki (2021) discussed different types of threats that an organization's information systems and data can face. As part of this work, they define the estimation of the MTD as a product of the BIA. According to Ruddin et al. (2021), disaster recovery planning should be conducted in nine stages, the seventh of which covers the consideration of financial and non-financial impact. The first limitation of the proposed process is that it is focused on a single industry and therefore does not account for the differences that might exist from one industry to another. Another limitation is that no provision informs a constant improvement process that takes updated system performance data as input. Finally, the process offered by Ruddin et al. (2021) is neither formalized nor standardized.

### 2.4.6. DRP of Data Systems for Indonesia University

With its basis on ISO 27031, an international standard that provides guidance for information and communication technology readiness for business continuity (ISO/IEC, 2011), Meilani, Arief, and Habibitullah (2019) designed a DRP for an Indonesian university's data systems. In this work, Meilani et al. (2019) detailed the types of risks that organizations' information systems face, however priorities relating to regulatory or public relations concerns were not addressed. Also, based on the risks acknowledged by Meilani et al. (2019), the RTO and RPO assessments performed have similar limitations. The results of the study conducted by Meilani et al. (2019) show a strong dependency on alternate sites as a DRP strategy. However, in the absence of a reliable failover system, or where backup data is required for when malware corrupts both primary and secondary systems, redundancy that is provided by having multiple sites does not offer reliable protection.

### 2.4.7. Regression-based Recovery Time Predictions

A process based on Regression Analysis techniques proposed by Podaras, Moirogiorgou, and Zervakis (2021) is intended to calculate a prediction of the recovery time for a given system. Podaras et al. (2021) also acknowledge Recovery Priorities as an integral part of Business Continuity Management. The model proposed offers a standard mathematical background for predicting the resumption time of business processes. It also features an inclusion of non-technical priorities for the estimation of recovery times. The model is an attempt to improve on the previously proposed model based on "business function recovery points" which are a collection of 46 business points of assessment that include human, technical, and environmental factors that influence recovery times. The proposed model calculates the Recovery Time Effort (RTE) which Meilani et al. (2019) defines as the total or summary of efforts required to recover a failed system. Podaras et al. (2021) claim that from the RTE the RTO can be deduced by anticipating unforeseen circumstances. Because this approach is proactive in nature, the extent to which unforeseen circumstances can affect a recovery process is unknown, and the possibilities can be infinite. Also, the model offers a one-time calculation of this estimate with no provision for future adjustments based on the history and performance of the organization’s information systems.

### 2.4.8. Security-Oriented Assessment Framework

The framework proposed by Luo et al. (2020) uses the AHP to determine the feasibility of the index systems for the perception layer of electric Internet of Things (IoT). The framework proposes the use of the China Standard in Global Technology GB/T 20988-

2007 to select RPO and RTO, which is then used to determine the data availability protection capability of perception layer of electric IoT. The Goubiao National Standard GB/T 20988-2007 only suggests a relationship between given ranges for both the RTO and RPO but does not offer a way to derive either metric.

### 2.4.9. Summary of proposed models

Table 2 is used to present a summary of the proposed models when analyzed using the following criteria:

a. Business-driven tolerance limit

b. Performance history-based adjustments

c. Objectives and tolerance relationship

d. Sub-system separation of functionality

e. Priority-based recovery decisions

Table 2. Summary of Previous Work

| ID. | Model/Solution | Criteria | | | | |
|---|---|---|---|---|---|---|
| | | a | b | c | d | e |
| 1 | Gap Time Reduction | ✓ | ✗ | ✓ | ✗ | ✗ |
| 2 | Multi-Objective Scenario-Based Stochastic Robust Optimization | ✗ | ✗ | ✗ | ✗ | ✗ |
| 3 | Smart Recovery Advisory | ✗ | ✓ | ✗ | ✗ | ✗ |
| 4 | Computer Aided Disaster Recovery Planning | ✗ | ✗ | ✗ | ✗ | ✗ |
| 5 | Digital Recording Company | ✓ | ✗ | ✗ | ✗ | ✓ |
| 6 | Indonesia University Study | ✓ | ✗ | ✗ | ✓ | ✗ |
| 7 | Regression Based Time Prediction | ✓ | ✗ | ✗ | ✗ | ✓ |
| 8 | Security-Oriented Assessment Framework | ✗ | ✗ | ✗ | ✗ | ✗ |

## 2.5.Conclusion of Literature Review and Research Gap

A review of the existing literature confirmed that there is yet to be a solution that establishes recovery time and data metrics (RTO and RPO) in a way that either agrees with the organization’s tolerance limits and technical capabilities or offers a process that factors the organization’s performance in previous assessments and drills into future decisions. As was seen earlier in the chapter, some solutions have been offered that improve economic efficiency in the decision-making process, prioritize organizational interests, and attempt to standardize their recovery approach. Others have offered models that estimate the recovery time in some cases, however, the considerations made in the process do not align with the preferences and concerns as expressed by the surveyed industry practitioners. Therefore, it is appropriate to conclude that neither prior research efforts nor previously proposed solutions have been aimed at establishing the metrics with which recovery objectives can be selected, assessed, or improved using data from a history of the system’s performance.

# CHAPTER 3
# PROCESS REQUIREMENTS

In this section, the requirements for a proposed solution are explored. The section starts with a description of the requirements that the potential solution will aim to meet. In the following sub-sections, relevant existing metrics are reviewed, and their relevance to the proposed solution is discussed. The section ends with the criteria and expectations of the survey questionnaire used to determine the rest of the organizational preferences and priorities that the variables used to develop the proposed solution are based on.

## 3.1. Solution Goals

The goals that a potential solution to the research problem will aim to meet are drawn directly from the criteria which were used to assess the previously proposed solutions. These goals are described below:

- The ability for an organization's tolerance limits, both with regards to restoration time and data loss, to be driven by business requirements in a manner that is independent of information technology infrastructure and management. This ensures that the limits of the organization's tolerance are not biased, and therefore not influenced by the preferences of the IT department.
- Periodic adjustments to the recovery objectives facilitated by the organization's schedule. This will allow the resulting recovery objectives to adapt to the organization's likely performance in a real incident.

- A clearly defined relationship between the resulting recovery objectives and the organization’s defined tolerance limits. The organization can therefore justify the margin by which the tolerance limit should exceed its recovery objectives
- The use of separate recovery objectives for each sub-system to allow for isolation of potential problems or bottlenecks
- The selection of restore points that protect the organization’s highest priorities even when it does not agree with the stated objectives.

## 3.2.Existing Metrics and Theories

The theories and concepts that are widely accepted in incident response and recovery are commonly used as variables in service continuity planning and are adopted in this research not only because of their universal acceptability, but also because of their definitive position on the timeline of cyber incident recovery planning. In the next few sub-sections these concepts are described.

### 3.2.1. Business Impact Analysis (BIA)

The Business Impact Analysis is a process, or the result of a process undergone by an organization to understand the consequences and impact that a given event will have on its value-creating processes (Taarup-Esbensen, 2020). This analysis defines the organization’s economic tolerable limits and can be performed in different ways and at different levels. Depending on the level and scope, it sometimes produces the Maximum Tolerable Downtime (MTD) (Ruddin, Santoso, Indrajit & Dazki, 2021), and can also produce the Recovery Objectives (RTO/RPO) (Atiku, Garba & Bade, 2021). In other cases, it utilizes these metrics to estimate the best- and worst-case scenarios depending on the extent to which the service level agreements defined by the recovery objectives are met. In this research, the BIA is referred to in order to obtain the MTD. Given that information technology staff are likely to have an incentive to increase the MTD, and for proper separation of responsibilities, it is beneficial for the BIA to be conducted independent of an organization's Information Technology department.

### 3.2.2. Maximum Tolerable Downtime (MTD)

The Maximum Tolerable Downtime as defined by Taarup-Esbensen (2020) is the point in the future beyond which the organization will no longer be able to sustain itself. This is the time which the impact of the event begins to have irreparable and unsustainable damage to the organization's ability to remain profitable. NIST (2021) also defines this variable or metric as the total amount of time the system owner/authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations. NIST (2021) further states that acknowledging the MTD is important because not doing so could leave contingency planners with imprecise direction on 1) selection of an appropriate recovery method, and 2) the depth of detail which will be required when developing recovery procedures, including their scope and content. Other names that have been used to define this metric are, Maximum Accepted Outage (MAO) (Suroso, Hamza & Sasongko, 2021) (Nejedlova & Podaras, 2017) and Maximum Tolerable Period of Disruption (MTPD) (Sahebjamnia et al., 2011).

### 3.2.3. Backup Frequency

The Backup Frequency defines how often a system is backed up or how often backup files are created. This cadence is normally defined by the organization according to their internal standards. In addition, although all frameworks studied by Goud (2019) highlight the importance of frequent backups, no general standards for the cadence and use of backups are proposed. According to Russell and Buffington (2021), a recent study conducted on preparedness revealed that 56% of backups taken will fail during restoration. The causes of most data restoration failures include human error, data corruption, and hardware component failure (Wang, Zhang & Xu, 2017). In another study, Goodwin (2021) reported that 43% of organizations suffered unrecoverable data in the past 12 months, and 63% of organizations have suffered a data-related business disruption within the past 12 months. These statistics further underscore the relevance of the backup frequency and overall backup strategy.

## 3.3. Survey Questionnaire

In the design and the development of the artifact, to establish and/or validate the variables used to create the model, a survey was conducted among qualified candidates, and the results were analyzed using quantitative methods to identify and validate the different pointers and key factors that are essential to organizations in recovery operations. The following are the criteria used for the selection of the participants of the survey:

- Have performed organizational duties or held a position in the capacity to make or contribute to strategic decisions involving cyber incident recovery
- Are between the ages of 25 and 65

The questionnaire used for this survey was reviewed and approved by the Institutional Review Board and was conducted according to the standards of the CITI program’s Research with Human Subjects (RCR). The results of the survey are presented in Chapter 4.

# CHAPTER 4
# RESEARCH METHODOLOGY

Due to the nature of this research and the expected outcome, the Design Science research methodology was used. This methodology would allow for the proposal and evaluation of a decision model that addresses the research problem directly. Peffers, Rothenberger, Tuunanen and Vaezi (2012) defined a “model” as a simplified representation of reality documented using a formal notation or language. According to Wieringa (2014) the artifact produced should interact with the problem context and aim to improve something in that context. This is validated along the way to justify its contribution to the research objective.

## 4.1. Research Processes and Steps

This research was conducted using the six-step process defined by Peffers et al. (2020) for Design Science Research. The six steps are as follows:

- Identification of Problem
- Identification of Research Objectives
- Design and Development of Artifact
- Fitment of the artifact with the problem context
- Evaluation of the artifact to determine utility, rigor, and efficacy
- Contribution to literature

Fig. 3. illustrates the overall process at a high level.

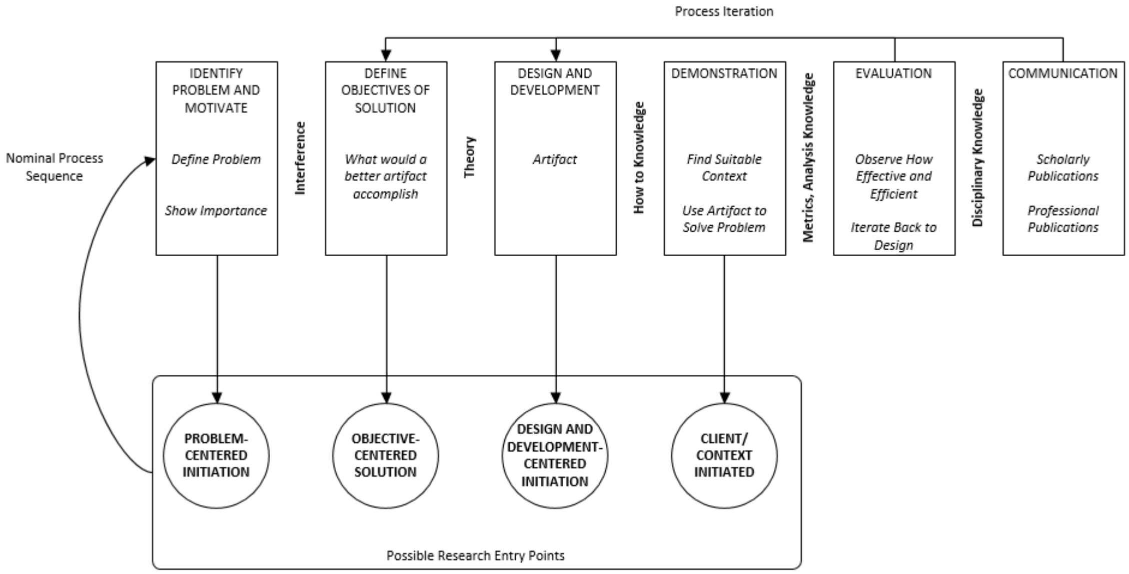

Process Iteration
Nominal Process Sequence
IDENTIFY PROBLEM AND MOTIVATE
Define Problem
Show Importance
Interference
DEFINE OBJECTIVES OF SOLUTION
What would a better artifact accomplish
Theory
DESIGN AND DEVELOPMENT
Artifact
How to Knowledge
DEMONSTRATION
Find Suitable Context
Use Artifact to Solve Problem
Metrics, Analysis Knowledge
EVALUATION
Observe How Effective and Efficient
Iterate Back to Design
Disciplinary Knowledge
COMMUNICATION
Scholarly Publications
Professional Publications
PROBLEM-CENTERED INITIATION
OBJECTIVE-CENTERED SOLUTION
DESIGN AND DEVELOPMENT-CENTERED INITIATION
CLIENT/ CONTEXT INITIATED
Possible Research Entry Points

Figure 3. Design Science Research Methodology (Peffers et al., 2020)

## 4.2.Demonstration

To demonstrate how the artifact works, the milestone events of a typical incident are placed on a timeline which is used to illustrate the relationship between the variables. The illustration makes use of realistic values for each variable to ensure that the context of the demonstration is suitable, and that the application of the artifact solved the problem. The illustration is depicted in Figure 6.

## 4.3. Evaluation Process

The evaluation of the artifact was conducted in four phases. First, a Numerical Experiment was conducted using data that is representative of a real-world incident. The numerical experiment was conducted to test the robustness of the artifact. Next, a Direct Comparison of the artifact with previously proposed models was made to highlight its differences and ability to address the research gap. An illustrative scenario based on real world circumstances and conditions as described by Wieringa (2014) was used in the following phase. This is due to the limited availability of details such as cause and effect, preparation level, resource deployment, and other organizational inner workings related to cyber incidents. Other contributors to the limited information on cyber incidents according to Romanosky (2016) include the absence of legislative and regulatory disclosure requirements, and concerns regarding privacy and organizational interests. To facilitate the demonstration of the artifact's efficacy, a synthetic environment was constructed. Finally, the artifact was presented to two experts for review, one from a technical perspective and the other from a business/financial perspective.

The evaluation of the artifact was intended to demonstrate the three attributes outlined by Veneble, Bakersville and Pries-Heje (2012) as listed below:

- Rigor – Shows an observable improvement and works in a real situation
- Efficiency – Can be performed within resource constraints
- Ethics – Does not endanger any entities in the process.

Also, due to the synthetic environment and the fact that the evaluation occurred after the construction of the artifact the evaluation is considered "Artificial" and "Ex-Post" in its nature (Veneble, Bakersville and Pries-Heje, 2012).

# CHAPTER 5
# DECISION MODEL

To address the arising question of how to establish recovery objectives (metrics) in a way that accounts for an organization's unique circumstances, the following model is proposed. This model can be applied to, and further developed for specific circumstances in an IT environment.

## 5.1. Description of the artifact

### 5.1.1. Variables

The variables were created using the results from the survey as outlined in the Process Requirements in Chapter 3.

### 5.1.2. Survey Responses

The questions in the survey questionnaire to which a total of 67 participants responded were designed to establish a position in the areas relevant to the research. The participants were selected from among qualified Information Technology professionals who met the criteria described in Chapter 3, Sub-section 3.3.

In Tables 3, 4, 5, and 6, the questions sent to the survey participants that are relevant to the creation of the decision model, along with the responses received showing the percentages and parameters for each question area are presented. A full list of all the question presented to the survey participants is available in Appendix C.

Table 3. Recovery Drills and Metrics

| Nº | Question | Percentage | Parameter |
|---|---|---|---|
| 2 | How often on average does your organization conduct recovery drills? | 70.15 | At least twice a year |
| 3 | How often do you meet or exceed recovery goals? | 37.31 | Always |
| | Table 3. Continued. | | |
| 5 | What Recovery Metrics do you use to measure success and/or failure to test your recovery capabilities? | 76.12 | RTO/RPO |
| 23 | Does your organization have an official declaration of disaster and start of the “recovery” clock? | 87.69 | Yes |

Table 4. AHP Criteria

| Nº | Question | Percentage | Parameter |
|---|---|---|---|
| 7 | Is your organization subject to any regulatory oversight? | 85.07 | Yes |
| 9 | Which of the following will a successful cyber-attack on your organization have the most impact on? | 91.05 | Confidentiality/ Integrity/ Availability |

Table 5. AHP Alternatives

| Nº | Question | Percentage | Parameter |
|---|---|---|---|
| 14 | On a scale of 1-5 (1=Lowest, 5=Highest) how much does “time of failure or breach” matter with regards to recovery objectives? | 83.08 | 3 or higher |
| 15 | On a scale of 1-5 (1=Lowest, 5=Highest) how important is the “time of discovery” of a breach or failure with regards to recovery objectives? | 89.24 | 3 or higher |
| 22 | Which of the following does your organization recognize for the purpose of recovery objectives? | 33.85 | Time of Impact |

Table 6. Sub-system Recovery

| Nº | Question | Percentage | Parameter |
|---|---|---|---|
| 11 | Which of the following best describes your recovery process? | 30.77 | Segmented, Tiered or Sequential |
| 12 | With regards to recovery, how do you best describe the relationship between the components or layers of your IT environment? | 98.46 | Staggered or Linear |
| 13 | If recovery of systems is layered, are there recovery objectives/metrics established separately for each layer, application, or system? | 75.38 | Yes |
| 18 | Do you have recovery objectives for each layer/subsystem (i.e., Database, Network, Applications), or a general set of objectives? | 50.77 | Separate |

The responses to the survey questionnaire were used to justify the creation of the following variables which became the foundation of the proposed artifact:

- $RTO_1$ – Lower limit of the Recovery Time Objective range
- $RTO_2$ – Upper limit of the Recovery Time Objective range
- RTO – Recovery Time Objective. The value selected as the target time for recovery operations
- RPO – Recovery Point Objective. The value selected as the restore point target for recovery operations
- tD – Time of Discovery. The time a breach or incident was first discovered
- tI – Time of Impact. The time an incident begins to impact an organization’s normal operations

- tB – Time of Breach. The exact time an information system is breached
- $t_n$ – Recovery time for each sub-system. “n” represents the number assigned to the sub-system or layer based on its hierarchy as illustrated in Table 1
- y – Excess Time. The margin by which recovery for each sub-system exceeds the established RTO
- T – Average Excess Time
- tA – Incident Declaration/Acknowledgement time
- tP – Timing Priority. Priority selected using AHP to determine the exact restore point.

### 5.1.3. Existing Metrics

The following variables used in the creation of the proposed model were identified as existing metrics and theories:

- F – Backup Frequency (as defined in sub-section 3.2.3)
- C – Maximum Consecutive Failures. The maximum number of times backups failed consecutively
- MTD – Maximum Tolerable Downtime (as defined in sub-section 3.2.2)
- BIA – Business Impact Analysis (as defined in sub-section 3.2.1).

### 5.1.4. Technical and Operational Gaps

Based on the technical dependencies among subsystems, the difference between the RPO and the expected Restore Point due to organizational priorities, and the time difference between the linear and staggered recovery process, the following variables are created:

- $W_n$ – Wait/Pause time for each sub-system. The total time from the beginning of the recovery operation that recovery of a sub-system is paused to allow for progress on dependencies.
- AR – Actual Recovery Target Time. The final restore point selected.
- Δ – Change. A change in total recovery time when a staggered recovery approach is used.

The expectation was that defining the arithmetic relationship between these variables (except the times of discovery, impact, and breach) in a manner that avoids overlaps will ensure that the resulting recovery objectives (RTO and RPO) do not fall outside the tolerable limits.

In the proposed decision model, a choice is made at some point in the process among tD, tI and tB, using the AHP, of which of the three is of highest importance. In this process, the goal was to select the right “Timing Priority” which is what determines the incident acknowledgement or declaration time *tA*. The Criteria are three of the most common motivations for establishing recovery metrics which are, regulatory requirements, stakeholder confidence, and economic impact, as noted by Podofillini, Wolfgang, Bruno and Bozidar (2015).

### 5.1.5. Overview and Concept

The proposed decision model is illustrated using the chart presented in Fig. 4. The process begins with determining the RTO boundaries. These are the upper and lower limits from within which the RTO can be selected and are represented as $RTO_2$ and $RTO_1$ respectively. The relationship between the upper limit ($RTO_2$) and the MTD is also defined, and the organization’s performance in recovery assessments is established as an input source for future updates to the RTO.

Next, the RPO is defined using the Backup Frequency which is represented as *F* as a primary input. It also considers the performance of previous backup operations with regards to failures. This history is factored into the RPO selection and update process to reflect the organization’s capabilities, highlight deficiencies, and reduce the chances of unexpected data loss.

Finally, the appropriate restore point based on the organization’s specific priorities is determined depending on what the driver of that priority is. This process involves using the Analytical Hierarchy Process (AHP) with Pair-Wise comparison techniques to select among alternatives given certain criteria.

Specifics of the artifact will vary from one application to another, as organizational needs, capabilities, budget, culture, and IT environment differ. However, the principles and overall concept are repeatable and transferable.

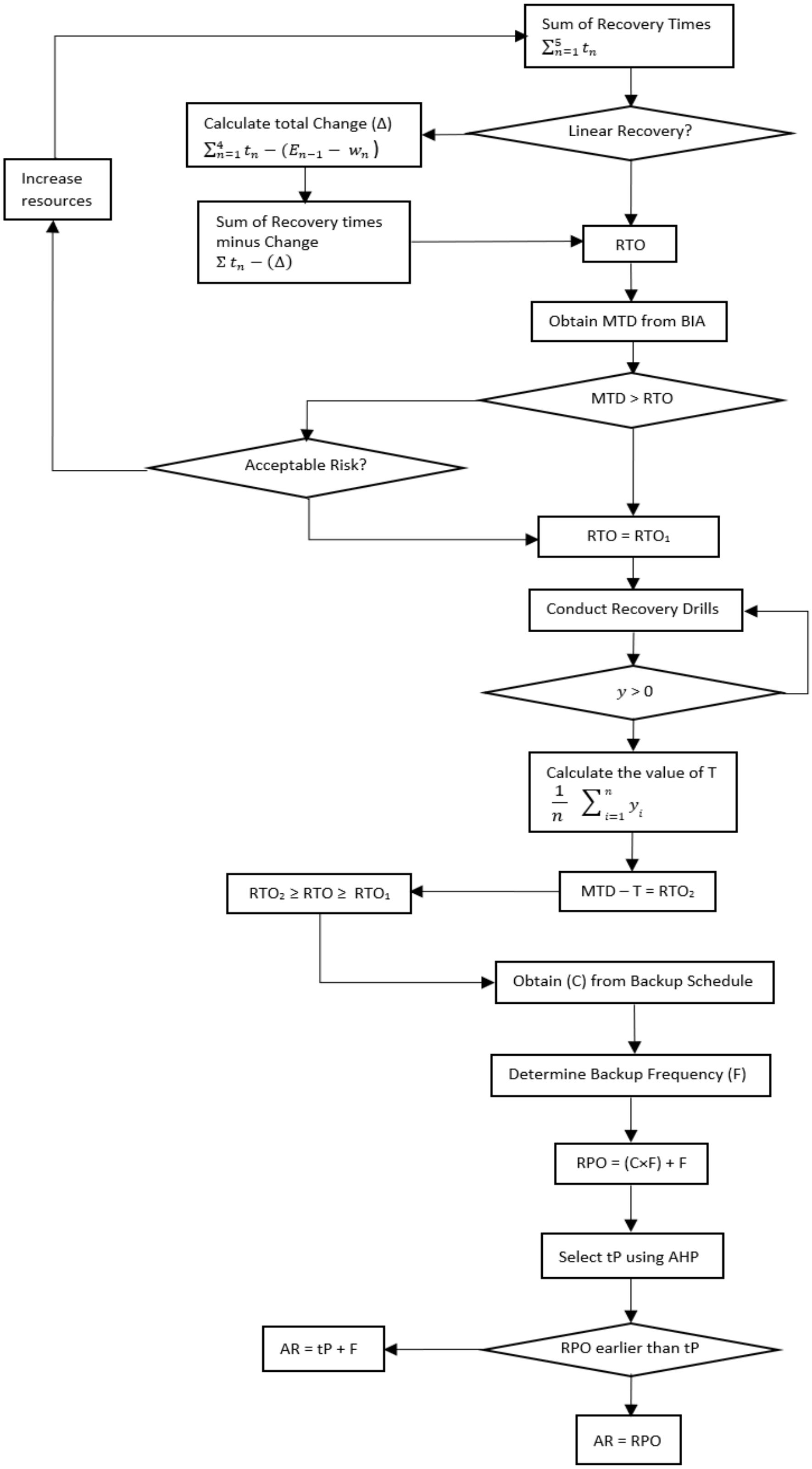


Figure 4. Decision Model

## 5.2. Details of the artifact

In the following steps, a detailed description of how the artifact will work if applied in a typical IT environment is discussed. It is noteworthy that the application and implementation may vary depending on specific organizational circumstances.

### 5.2.1. Defining Restore Time Boundaries – Deriving RTO$_1$

The process for setting the RTO range involves identifying two boundaries which form the RTO range. In this model, the RTO is not a single metric but rather a variable that falls within the range defined by a maximum (RTO$_2$) and a minimum (RTO$_1$) limit. Both values are calculated independently. The first step in the model is to determine the value of RTO$_1$ which is given by an aggregate or sum of the recovery times of all the sub-systems.

A distinction is made between systems that are recovered in a "linear" fashion, which is where the recovery of one sub-system must be completed before work on the next one in the hierarchy is started, or if a "staggered" approach is used where recovery of several subsystems can be started simultaneously. If the recovery process is linear then RTO$_1$ is calculated as follows:

$$RTO_1 = \sum_{n=1}^{5} t_n \qquad (3)$$

If the approach for deploying recovery resources is not linear, and work can start on different parts of the system simultaneously, then based on the inter-dependencies among the subsystems or layers, the total time saved by starting work simultaneously is calculated as "Change" Δ and deducted from the total of all recovery times to obtain RTO$_1$. This is achieved in two steps:

*a)* Calculate the total time saved, or change in time (Δ) using the formula in equation 4:

$$\sum_{n=1}^{4} t_n - (E_{n-1} - w_n) \quad (4)$$

*b)* Deduct the results in step a) from the sum of all recovery times using the formula below:

$$\Sigma\, t_n - \Delta \quad (5)$$

The results of the above becomes the $RTO_1$ for a system where a staggered approach is used.

To test its validity, $RTO_1$ is compared with the MTD. In this model, it is suggested that the MTD is obtained from the organization's Business Impact Analysis as Taarup-Esbensen (2020) and Ruddin et al. (2021) noted. If $RTO_1$ is smaller than the MTD, it becomes the lower limit of the RTO range. If it is larger than the MTD, it is recognized as a risk and the appropriate treatment is applied (Samimi, 2020). National Institute of Standards and Technology (2011) defines the risk treatment activities as follows:

- Acceptance – The risk is accepted and documented, usually if the cost-benefit analysis is not in favor of any other treatment
- Avoidance – The entire activity is avoided. This treatment would not be applicable if there is a requirement to establish valid recovery objectives
- Mitigation – The risk is addressed directly to eliminate or reduce it, and
- Transference – The consequences of the risk are transferred or shared with another entity (NIST, 2011).

### 5.2.2. Defining Restore Time Boundaries – Deriving $RTO_2$

The upper limit or maximum value of the RTO range ($RTO_2$) is established by defining a direct relationship with the MTD.

Another variable used in the calculation of $RTO_2$ is the Average Excess Time denoted by *T*. During recovery drills or actual incidents, as established in the results of the survey, many organizations exceed their RTOs. This model proposes that the MTD should exceed $RTO_2$ by a minimum of the average margin by which the RTO has been exceeded during these drills. In this model, the “Excess Time” variable, denoted as “y,” defines the margin by which the recovery time for each system in a drill or event exceeds the RTO. Therefore, *$RTO_2$* is expressed as follows:

$$RTO_2 = MTD - T \tag{6}$$

$$\textit{where } T = \frac{1}{n} \sum_{i=1}^{n} y_i \tag{7}$$

Although noted by Podaras, Klara and Jiri (2016), recovery drills are presupposed in organizational recovery planning strategy. However, if a drill or assessment has not been conducted, and this model is being applied in the first attempt at establishing recovery objectives, then $RTO_1$ can be used as the RTO. Once both limits of the RTO range have been identified, they will define the limits from within which the RTO can then be safely selected.

To confirm that the selected RTO is within safe limits, the model proposes verifying that $RTO_2$ is greater or equal to the selected RTO, and also that the selected RTO is greater or equal to $RTO_1$ as expressed in equation 8.

$$RTO_2 \geq RTO \geq RTO_1 \tag{8}$$

### 5.2.3. Defining The Restore Point – Deriving RPO

Due to the complexity of the compression algorithms used in backup operations, they are prone to frequent failures (Russell & Buffington, 2021). This model proposes that the RPO should be greater than the Backup Frequency and should also consider the number of times the creation of reliable backup copies was not successful. This consideration can be done either with reference to the organization's own history, or external statistical data.

The model further proposes that for the RPO, the Backup Frequency or Cadence denoted as *F* is multiplied by the number of consecutive times a backup operation has failed to produce usable backup data, as acknowledged by Russell and Buffington (2021), which is denoted as *C*, and added to the value of *F*. This guarantees that there is one copy of the backup for when there is no failure and at least one iteration of the backup to compensate for each possibility of a failure based on the system's history. The resulting formula for calculating the RPO is expressed in equation 9.

$$RPO = F + (CF) \tag{9}$$

Multiplying the number of consecutive failures with the backup frequency accounts for the possibility that the backups could fail that same number of times, and adding it to another instance of the backup frequency allows the recovery operation to go back one more cycle due to the lack of availability of data resulting from consecutive failures. The relationship between these variables and metrics is illustrated in Fig. 6.

#### 5.2.4. Defining The Restore Point – Setting the Actual Recovery Target Time

The model concludes with a third variable defined as Actual Recovery Target Time denoted as *AR*. *AR* defines the restore point to which recovery operations should be targeted and explores its relationship with the RPO. The process begins with properly timing the incident by determining whether the time of breach *tB*, the time of impact *tI* or time of discovery *tD* is of the highest priority to the organization. This decision is usually influenced by such things as organization culture, regulatory requirements, and the economic impact of the incident, as confirmed using data from the survey. The model proposes the use of the Analytical Hierarchy Process (AHP) to make this selection.

The proposed Analytical Hierarchy Process (AHP) is the tool used to make the selection based on the organization's culture, preferences, and circumstances among the three variables, *tI*, *tD*, and *tB*. This selection is based on one of three criteria that most closely aligns with the primary motivations for setting recovery objectives. From the results of the survey that was conducted to determine organizational preferences and concerns, the criteria used in the AHP selection process were identified as "Regulatory Requirement," "Economic Impact," and "Organization Principle/Culture." Figure 5 illustrates the structure and specific application of AHP.

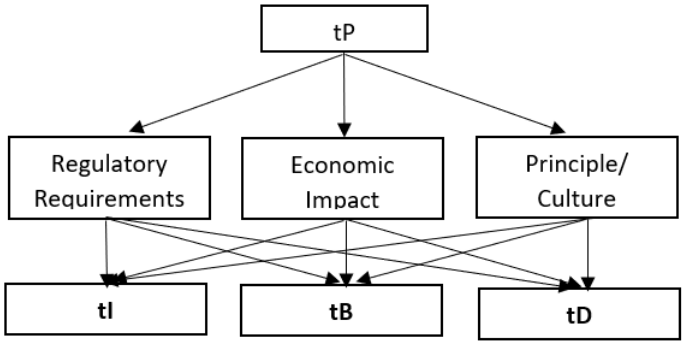


Figure 5. AHP Model

In the next step, another decision is made. The established RPO is compared to the time determined by the incident timing priority *tP* using AHP. If the RPO exceeds or is earlier than the established incident timing denoted as *tP* in the model, then recovery can be targeted to the time established by the RPO. On the other hand, if the RPO is later than the time established by *tP*, then an hour before the value established by *tP* is selected in lieu of the RPO as the recovery target time, and can then suffice as the reason or explanation for not meeting the RPO. The rationale behind the extra hour is to place *AR* at a time earlier than the value of *tP* in which case the last available and reliable backup data will be used for the restoration.

### 5.2.5. Summary

Based on the relationship between the MTD and the RTO, and that between the RPO and Backup Frequency *F*, two different formulae are proposed to derive these metrics objectively in such a way that ensures no overlaps, and is both repeatable and adaptable. The relationships are expressed as follows:

$$RTO_1 \geq RTO \leq RTO_2 < MTD$$

$$RPO = F + (C \times F)$$

## 5.3. Timeline Illustration

The next few sections show how each of the variables are derived and in what calculations they are used. In Fig. 6, sample numbers are used to graphically illustrate the relationship between the variables on a timeline.

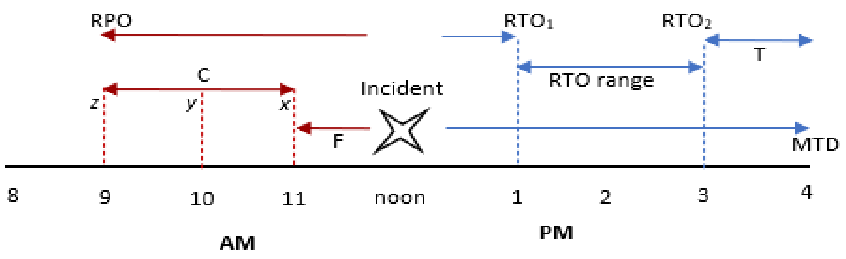


Figure 6. Incident Timeline

In the example presented in Fig. 6, an incident occurs and is declared at 12 noon [which is the tA] at an organization with an MTD of 4 hours. In this example, it takes about 1 hour to restore all systems, and in the past the organization has exceeded this time by an average of 1 hour. Based on this, the feasible RTO for the organization is between 1 and 3 hours.

The RPO on the other hand is calculated at 3 hours even though a backup is taken every hour. The additional time comes from the history of backup failures. The figure reflects that there have been about 2 consecutive backup failures in the recent past. Point x is the appropriate restore point if there were no failures. Point y and z are the restore points if there had been 1 or 2 consecutive failures respectively. This assures that the restore point established by the selected RPO accounts for the risk of a backup failure.

The RPO should be dependent on the Backup Frequency. This provides the assurance that the RPO is not set outside of the capabilities of the system and resources. Testing a system's recoverability and recovery capabilities using correct, feasible and realistic metrics paint a more accurate picture of what the likely results will be in the event of an actual incident.

Depending on what the motivation for setting recovery objectives and metrics is, in the event of an actual incident where system recovery becomes necessary, an organization must decide what point to recover the systems to. If the Time of Breach tB which is the time the system got compromised is more important to the organization, then recovery should be targeted to an earlier time to ensure that the status of the compromised system is not carried over into the recovered system. If the time when the incident begins to impact the organization (Time of Impact 'tI'), or the time the incident is discovered (Time of Discovery 'tD') is more of a priority to the organization, then the system should be recovered to a time that reflects this preference. The time the system is recovered to is recognized in this model as the Actual Recovery Target Time (AR) which can then be expressed as follows:

$$\textit{If} \qquad (RPO > tP)$$

$$AR = RPO \tag{10}$$

$$Else \quad AR = tP - 1 \tag{11}$$

In the above expression, if the calculated RPO is greater than the Time of Impact, Discovery, or Breach [depending on the organization’s priorities,] then AR is equal to the RPO. If this is not the case, then the AR should reflect the organization’s priorities with regards to timing the incident as well as the available recovery data.

# CHAPTER 6
# EVALUATION

The artifact was evaluated to test its ability to address the research problem and attain the research goal if implemented. As stated earlier, Wieringa (2014) describes Artifact Evaluation as the process of investigating the effects of an interaction between the artifact and a model of the problem context. Based on this interaction and its effects, a "design theory" was constructed for the purpose of predicting the effect of the implementation of the artifact in a real-world scenario. Wieringa (2014) describes design theory as a theory of the properties of the artifact and its interaction with the problem context.

The Evaluation then concluded using four different methods to validate the usefulness and efficacy of the artifact. First, a numerical experiment was conducted to demonstrate how the artifact can be used to define the parameters for the selection of recovery objectives based on the system's performance. Secondly, a direct comparison of the artifact's features and those of other previously proffered models was done to highlight the differences. Thirdly, the artifact was applied in an illustrative scenario using real world data, and the result of that application was validated based on the available data. Finally, the artifact was presented to two experts, both of whom participated in the initial survey. One of the experts gave a review of the artifact from a technical perspective, and the other gave a review from a business process and operations perspective.

## 6.1. Numerical Experiment

The environment for the Numerical Experiment was designed using experimental hypothetical data that is representative of a real-world context. This is due, both to the limited availability of real-world data and the amount of time and resources that would be required for a real-world experiment.

In the scenario used for this evaluation, the organization is an energy and utilities company that is regulated by the North American Energy Reliability Commission (NERC) which requires that an organization identify when the incident is first detected (Baham, Calderon & Hirschheim, 2017). In the scenario, the MTD is determined in the BIA to be 6 hours, and the organization conducts recovery drills every quarter, which exceeds the annual requirements as outlined by (Baham et al., 2017). Table 7 shows the recovery times that were presumed each time the recovery drills were conducted over the past year. In Table 7 each Period equals one quarter of the year, and the four quarters are represented by Q1 – Q4.

Table 7. Recovery Drills History

| **Period** | **Total Recovery Times (hr.)** |
|---|---|
| Q1 | 6 |
| Q2 | 5.5 |
| Q3 | 4 |
| Q4 | 5 |

The organization in the scenario backs up its systems and data every hour and has had three consecutive backup failures in the last twelve backup cycles. It also indicated that based on regulatory requirements, the time an incident is discovered is of higher priority than either the time it begins to have serious impact or the time the system was breached. The organization also indicated that the time of impact was of the lowest priority.

According to the scenario, on a given day, the IT staff reported for work at 7:30 am, and at 8:00 am some indicators of compromise were noticed. Some server names had been changed and there was unusual outbound network traffic. At 10:00 am, users began reporting that some critical applications and services were either unavailable or running slow. Their IT team launched an investigation, and forensic evidence indicated that malware had entered the IT environment at 6:00 am. The investigation also concluded that despite their vulnerability and susceptibility to injection-based attacks as described by Xu and Qian (2015) no external supporting network infrastructure was impacted.

As part of the design theory and for this evaluation, variables are provided in the table below for the recovery times for each of the subsystems of the IT infrastructure. At this point in the scenario, recovery objectives have not previously been established and the numbers in Table 8 are obtained from the IT department's estimate in their playbooks and runbooks.

Table 8. Recovery Data for Subsystems

| **Assigned Variable** | **Subsystem** | **Recovery Time (hr.)** | **Wait Time (hr.)** |
|---|---|---|---|
| $t_1$ | Storage | 1 | N/A |
| $t_2$ | Compute | 2 | 0 |
| $t_3$ | Network | 1.5 | 1 |
| $t_4$ | Database | 1 | 2 |
| $t_5$ | Application | 2 | 2.5 |

### 6.1.1. Recovery Time

For the Recovery Time Objective, the model proposes setting boundaries within which a valid RTO can be selected. To define these boundaries, an organization's best capabilities define the lower limit of the range ($RTO_1$), and its performance in the most recent drills or assessments is used to define the upper limit ($RTO_2$).

Using the data from the scenario, the RTO for a "linear" recovery process where the recovery of one subsystem must be completed before the next one begins is calculated using equation 3 as follows:

$$
\begin{aligned}
RTO_1 &= \textstyle\sum_{n=1}^{5} t_n \\
&= (1 + 2 + 1.5 + 1 + 2)\ hrs. \\
&= 7.5\ hrs.
\end{aligned}
$$

The Linear recovery process produces a minimum RTO of 7.5 hours which is greater than the MTD of 6 hours. A graphical representation is presented in Fig. 7.

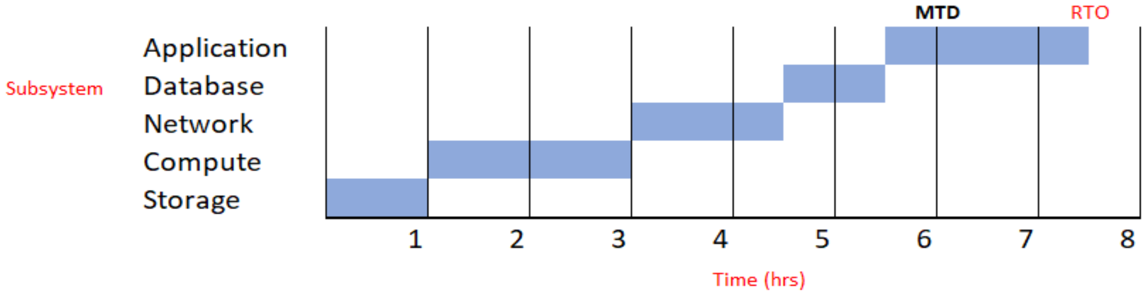


Figure 7. Linear Recovery Process

Using the same data from table 8, if a "staggered" recovery process is used, recovery of each subsystem can be performed simultaneously where applicable. However, due to technical dependencies, finalization of the recovery of a subsystem can only be completed after recovery of the preceding subsystem has been completed and tested. This gives rise to the wait/pause times denoted by *W*. RTO$_2$ is thus calculated by deducting the sum of the wait/pause times of each subsystem from the elapsed recovery time of the previous subsystem denoted by *E* and summing the results as expressed in equation 5.

The first step in calculating the RTO is to calculate the total change using equation 4 as follows:

$$\Delta = \sum_{n=1}^{4} (E_{n-1} - w_n)$$

$$= (3 - 2.5) + (2.5 - 2) + (2 - 1) + (1 - 0)$$

$$= 3\ hrs.$$

In the next step, to obtain the total recovery time using the staggered process, the change in time (Δ) is deducted from the sum of all individual recovery times.

$$RTO_1 = 7.5\ hrs. - 3hrs.$$

$$= 4.5\ hrs.$$

Based on the above, the total recovery time and therefore Recovery Objective is 4.5 hrs. This is illustrated in Fig. 8.

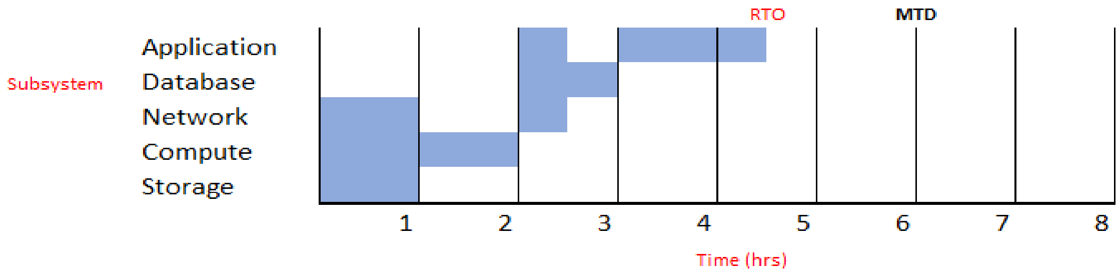


Figure 8. Staggered Recovery Process

In the above demonstration, an assumption is made that the organization did not previously have an RTO and was attempting to create one for the first time. The results show that if a linear or sequential recovery process is used, the RTO would be calculated as 7.5 hours, in which case, additional attention should be paid to reduce it as it exceeds the MTD. However, if the organization used a staggered recovery method, the resulting RTO would be

4.5 hours which is less than the MTD, and depending on the organization's preferences, further action might not be required. This also means that the organization will not have a value for the upper limit of the RTO range ($RTO_2$) at this point. The process for deriving this value is demonstrated next.

If the organization uses a staggered recovery approach as presented in the second example, the value for the average excess time denoted by *T* is derived by calculating the average of the Excess Times denoted by *y*. This then becomes the margin by which the Maximum Tolerable Downtime should exceed the RTO. As expressed in equation 6 this is calculated as follows:

$$\begin{aligned} T &= (y_1 + y_2 + y_3 + y_4) \div 4 \\ &= (1.5 + 1 + 0 + 0.5) \div 4 \\ &= 3 \div 4 \\ &= 0.75 \end{aligned}$$

It is noteworthy that the recovery time for Q3 is set to zero as it does not constitute an "overage" or an instance where the RTO is exceeded. This is because the Total Recovery Time for this period (4 hours) is less than the established RTO (4.5 hours). Further, it is shown that the recovery times for each sub-system exceed the established RTO by an average of 0.75 hours. This means that the upper limit or maximum value of the RTO ($RTO_2$) is calculated as follows, using equation 6:

$$\begin{aligned} &MTD - T \\ &= 6 \text{ hours} - 0.75 \text{ hours} \\ &= 5.25 \text{ hours} \end{aligned}$$

Based on the above example, the range to safely establish the RTO is between 4.5 hrs. and 5.25 hrs. This demonstrates that if the RTO is set to a value below 4.5 hours, the objective is not likely to be met. Similarly, if it is set to a value higher than 5.25 hours, there is a greater risk of exceeding the MTD putting the organization in greater proximity of the risk defined in the BIA.

### 6.1.2. Recovery Point

The first step in establishing the RPO was to obtain the Backup Frequency *F* and the Maximum Consecutive Failure *C* variables from the backup schedule. Using this information, and based on the given scenario, the RPO was calculated as defined in equation (7), as follows:

$$\begin{aligned} RPO &= FC + F \\ &= 3\ hours + 1\ hours \\ &= 4\ hours \end{aligned}$$

Being that the RPO is only an objective and not an actual representation of the system's capabilities, in the event of a failure, it is expected that the system could be restored to any point in time that is less than or equal to the 4 hours preceding the acknowledgement time of 12 pm in the scenario. During this evaluation, the proposal on how to establish the RPO presented a new challenge which required determining the process of acknowledgement of the incident. This was an essential element in the determination of the RPO because it sets the starting point from which to work backwards.

As organizations differ in how they acknowledge and address incidents, due to the influence the time of acknowledgement has on the recovery objectives, three variables were established and reaffirmed as viable options for making the distinction. The decision model further proposes the use of a multicriteria decision process to select which of these three valuables is best suited for the organization's needs, and then base the "Actual Recovery Target Time," which is the time the systems and data are recovered to, on the selected option.

Using the process illustrated in Fig. 5 along with Pairwise Comparison techniques, an exact priority time for the incident can be derived and recognized by the organization. This value becomes the basis for determining the Actual Recovery Target Time *AR* and justifying a stray from the RPO if necessary.

To perform the Pair-Wise Comparison for the three alternatives based on the organization's responses according to the scenario, the following scale of relative importance is constructed using Saaty's method (Saaty, 1987). Tables 9, 10 and 11 present the Scale of Relative Importance, Pair Wise Comparison details, and the Normalized Pair Wise Comparison respectively.

Table 9. Scale of Relative Importance

| **Alternative** | **Value** | **Description** |
|---|---|---|
| tI | 1 | Equal Importance |
| tB | 3 | Strong Importance |
| tD | 5 | Extreme Importance |
| N/A | 2, 4 | Intermediate Values |

Table 10. Pair Wise Comparison

| | **tI** | **tD** | **tB** |
|---|---|---|---|
| tI | 1 | 1/5 = 0.2 | 1/3 = 0.33 |
| tD | 5 | 1 | 1/3 = 0.33 |

Table 10 - Continued

| | | | |
|---|---|---|---|
| tB | 3 | 3/5 = 0.6 | 1 |
| Sum | 9 | 1.8 | 3 |

Table 11. Normalized Pair Wise Comparison

| | **tI** | **tD** | **tB** | **Weights** |
|---|---|---|---|---|
| tI | 1/9 = 0.11 | 0.2/1.8 – 0.11 | 0.33/3 = 0.11 | 0.33/3 = 0.11 |
| tD | 5/9 = 0.56 | 1/1.8 = 0.56 | 1.66/3 = 0.55 | 1.67/3 = 0.56 |
| tB | 3/9 = 0.33 | 0.6/1.8 = 0.33 | 1/3 = 0.33 | 0.99/3 = 0.33 |

From the above analysis, the time of discovery *tD* has the highest weight and therefore will be used to determine the target recovery point *AR*.

To demonstrate how this would work in the real world, the same scenario presented in the evaluation of the Recovery Point is used. In this scenario, the system is breached at 6:00 am, the breach is discovered at 8:00 am, and the system begins to lose functionality at 10:00 am. Using the organization’s priority in incident recognition as computed with the AHP, and the RPO as inputs, the actual recovery target time *AR* was calculated for each of the three possible outcomes.

From the decision model, three different calculations were made to determine whether the RPO placed the recovery target time earlier than the three possible values of the incident acknowledgement priority. In the cases where the RPO landed at a later time, the time determined by the Incident Priority time was reduced by one hour to establish a value for *AR* that was earlier and would therefore satisfy the organization’s recovery priorities.

## 6.2. Direct Comparison

In the second part of the evaluation, a direct comparison of the artifact with the previously proposed models and solutions is done to highlight the differences and the features of the artifact that have so far not been offered previously. Table 12 below is used to illustrate:

Table 12. Direct Comparison

| Solution | Business Driven Tolerance | Performance Based Adjustments | Objectives/ Tolerance Relationship | Sub-system Separation | Priority Based Decisions |
|---|---|---|---|---|---|
| Gap time Reduction | Yes | No | Yes | No | No |
| Multi-Objective Scenario-Based Stochastic Optimization | No | No | No | No | No |
| Smart Recovery Advisor | No | Yes | No | No | No |
| Computer Aided Disaster Recovery Planning | No | No | No | No | No |
| Digital Recording Company | Yes | No | No | No | Yes |
| Indonesia University Study | Yes | No | No | Yes | No |

Table 12 - Continued

| | | | | | |
|---|---|---|---|---|---|
| Regression Based Time Prediction | Yes | No | No | No | Yes |
| Security -Oriented Assessment Framework | No | No | No | No | No |
| Our Model | Yes | Yes | Yes | Yes | Yes |

## 6.3. Illustrative Scenario (real-world data)

The evaluation method employed in this part of the evaluation is Illustrative Scenario. Peffers, Rothenberger, Tuunanen and Vaezi (2012) defined this as the application of an artifact to a synthetic or real-world situation aimed at illustrating the rigor and suitability or utility of the artifact. Data from two recent independent global studies were used to create a context in which the artifact was applied. The results were then compared with suggestions made in a third study.

Russell and Buffington (2021), in a recent study found that 58% of recovery operations from backups fail due to a combination of failed backups and failed restore capabilities. Goodwin (2021) also found that the average backup schedule has a backup frequency of 24 hours. Given these two data points, the number of failed backups that can be assumed in a two-week period is calculated as follows:

$$58\% \times 14 = 8.12$$

$$\cong 8$$

With approximately 8 failed backups in a two-week period, even with the most even distribution of those failures, the minimum number of consecutive failures is 2. This means that if the artifact is applied in the same context in which both studies were conducted, the RPO would be calculated as follows using equation 9:

$$\begin{aligned} RPO &= FC + F \\ &= (24\times2) + 24 \\ &= 48 + 24 \\ &= 72 \text{ (3 days)} \end{aligned}$$

## 6.4. Results

### 6.4.1. Numerical Experiment

In the first part of the evaluation, the RTO range was calculated. This was illustrated as the range between the values of $RTO_1$ and $RTO_2$. Using a Linear recovery process results in a longer overall recovery time. In the evaluation, this caused the recovery time to exceed the MTD and the conflict was immediately obvious. Switching to the staggered method produced a lower minimum $RTO_1$ value. Table 13 is used to illustrate the results, and all values are expressed in hours.

Table 13. RTO Final Analysis

| | **MTD** | **$RTO_1$** | **Margin** | **$RTO_2$** | **Range** |
|---|---|---|---|---|---|
| Linear | 6 | 7.5 | -1.5 | - | - |
| Staggered | 6 | 4.5 | 1.5 | 5 | 0.5 |
| Change | N/A | 3 | - | - | - |

The results in Table 13 show a positive change of 3 hours in the value of $RTO_1$ moving from a linear to a staggered method. It also shows a range of 0.75 hours (4.5 hours to 5.25 hours) within which the RTO can be selected. This means that an RTO no less than 4.5 hours and no more than 5.25 hours can be safely used.

The second part of the numerical experiment tested the process for establishing a reliable recovery point. In this part of the test, two variables were realized, the RPO and the AR. The RPO of 4 hours was achieved by multiplying the highest consecutive number of backup failures *C* by the backup frequency *F and* adding a single value of the backup frequency *F* to the result. This demonstrates that the system can be expected to be restored using the most recent backup if there were no failures, and that every additional consecutive failure creates additional risk of not having a reliable backup with which to restore the system. Consideration of this risk was used to justify moving the RPO further backwards on the recovery timeline.

The Actual Restore Point was determined by using the multicriteria decision process AHP to select an incident timing priority on the timeline. This was used to determine the specific recovery target time. In the demonstration above, the incident discovery time *tD* had the highest priority and was used to determine the actual restore point. This means that *AR* will be resolved to one hour earlier than the time of discovery, which is 7:00 am.

### 6.4.2. Comparison with Similar Work

In the next part of the evaluation, the decision model was compared to previously proposed models identified in the literature review. The results demonstrated the decision model’s efficacy in the five assessment areas. A brief discussion of its applicability and utility is presented in the sub-sections below.

### *Business Driven Tolerance Limit*

The artifact features a step in which the organization’s maximum tolerance limit is obtained directly from the BIA to establish the MTD, and not created as part of its functionality. Obtaining this value from an entity outside the IT department ensures that there is no bias or preferential considerations made in the process. Testing the organization’s capabilities against this threshold also increases the quality and reliability of the results.

### *Performance-based Adjustments*

The selection of recovery objectives is usually the responsibility of an organization’s Information Technology leadership, except when other departments are affected in one way or the other, whereby a collaboration with the affected departments might become necessary. An organization’s success or failure in system recovery activities is largely based on their ability to meet their recovery objectives. Therefore, adjusting them accordingly, with input from the details that reflect the organization’s recent performance in assessments, allows the organization to align its decisions with its capabilities.

To satisfy this, the proposed decision model features the reuse of data from recovery assessments and drills to calculate the “buffer” between the upper limit of the RTO ($RTO_2$) and the MTD. Similarly, in determining the RPO, the decision model factors the “consecutive” backup failures into the likelihood that reliable backup data will be available and allows for the adjustment of the RTO based on that.

### *Objectives and Tolerance Relationship*

Clarifying the arithmetic relationship between the recovery objectives and the organization’s tolerance limits with regards to recovery time will help ensure that the tolerance limits such as the MTD will not be exceeded (Kawaguchi, 2013), and that recovery can be completed in a timeframe less than the MTD (Taarup-Esbensen, 2020). In a previous model proposed by Kawaguchi (2013), the “gap time” between the “Current Recovery Time (CRT)” and the MTD is used to determine the RTO. This forced a focus on the relationship between the CRT and the RTO. Other proposals offer the MTD and RTO as products of the BIA but offer no succinct selection process.

The proposed model improves the process by using a system’s performance and history relating to recovery time to estimate the likelihood and extent to which a recovery time target might be exceeded, and selecting an RTO that reflects this estimation, thereby redirecting the focus, if necessary, on the MTD and RTO relationship.

### ***Sub-system Separation of Functionality***

Taarup-Esbensen (2020) acknowledges the importance of identifying the interdependencies’ critical processes, as well as recognizing their recovery times separately. Principles such as separation of duties and responsibilities can give rise to this in some organizations. In the survey that was conducted to establish organizations’ priorities 44.78% of the participants confirmed that their organizations have different recovery objectives for each subsystem. In the context of cyber incident recovery, and in view of the fact that different types of cyber-attacks target and impact different sub-systems, a separate but similar set of recovery objectives can thus be justified.

### ***Priority-based recovery decisions***

Recognition of the organization’s priorities as proposed by the model is based on the three criteria identified as influential in the organization’s decision-making process regarding response and recovery from cyber incidents. These criteria were also confirmed in the survey questionnaire as outlined in the Process Requirements chapter.

### 6.4.3. Illustrative Scenario

The artifact was applied in an illustrative scenario based on real world data, and the resulting minimum RPO was 3 days (72 hours). This is based on an average 24-hour backup frequency and a 58% backup failure rate. This result is also confirmed by the data presented by Thomas et al. (2018) shown in table 14, which is based on NIST SP 800-30. This means that, as confirmed by the application of the artifact and confirmed by Thomas et al. (2018), the average RPO for most organizations should be around 3 hours. Although the demonstration resulted in a 3-hour RPO, based on the design of the artifact, its recommendation for recovery objectives is flexible and can change, based on the performance of the system.

Table 14. Information Security Assessment Backup Evaluation Guide

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| Backup Factor | General Guidance | Success Criteria | Findings | Recommendations |
| Backup Paradigm | Does the backup paradigm allow full point-in-time restores? | The system must be able to restore fully to the previous state on a given day. | | |
| RPO Capability | How far back can the backup system create a previous state? | Minimal = 3 days, Conservative = 14 days, Aggressive = 21 days | | |
| Backup Server Access | Who can access the backup server? | Only backup administrators or those with legitimate need should be able to access | | |
| Backup Server Network Connections | Which systems can be connected to the backup system? | The backup systems should be isolated, and only systems with need should be able to be connected. | | |

Table 14 - Continued

| | | |
|---|---|---|
| Backup Server Storage | Can the backup storage systems be shared? | Backup system storage system sharing should be limited. Other systems should not be used as a “bridge” where unintended users can write to the backup systems. |

*Note.* From “Improving Backup Systems Evaluations in Information Security Risk Assessments to Combat Ransomware,” by J. Thomas and G. C. Galligher, 2018, *Computer and Information Science* CCSENET Journal 11(1), p.23 (https://doi.org/10.5539/cls.v11n1p14

### 6.4.4. Expert Opinion

In the fourth and final part of the evaluation expert opinion was sought from two experts for review and evaluation. One gave a technical perspective and the other gave a business process perspective. The expert who provided the technical evaluation is experienced in the field of disaster recovery and incident response planning and has worked in several global organizations in leadership capacity providing consultative and advisory oversight at the organizational leadership level. Below is the statement issued after the evaluation:

> *Few will deny that digital resilience is today, in fact, business resilience. Digitally resilient organizations will continue to provide service to customers and stakeholders in the event of an interruption to normal operations including the business being affected by a “disaster.” Digitally resilient organizations maintain reputation and competitiveness in spite of being impacted by today’s disasters which are primarily cyber incidents.*

> *Organizational efforts to achieve resilience fail mainly because business and technology have difficulty establishing common goals to establish, fund, and maintain appropriate organizational disaster recovery responses. In simple practice, organizations typically established a single point RTO and RPO, conducted a test, and waited for a readiness grade based upon those two factors.*
>
> *The proposed model with its ability to establish multiple views of RTO and RPO will foster more open engagement between business and technology as it can be used to be more effective in relating to actual business operating requirements. By doing so, business and technology can better understand the organizational resilience requirements and establish effective recovery workbooks. Preparation for the ubiquitous threat to any organization requires a high level of understanding and active collaboration between business and technology.*
>
> *This new model provides a new and flexible approach for collaboration. The traditional and staggered recovery approaches can be managed to set a course for technology to recover the business organization flexibly as it responds to cyber incidents and assures organizational resilience.*

The second expert evaluation was given from a business process perspective with financial considerations. The expert who performed the review is proficient in finance and enterprise performance and has operated in that capacity for over twelve years. The following statement was issued as part of the evaluation:

> *After thorough review of the proposed artifact, I believe that it will be highly impactful if implemented in a real-world setting. If implemented, a trigger / alert*

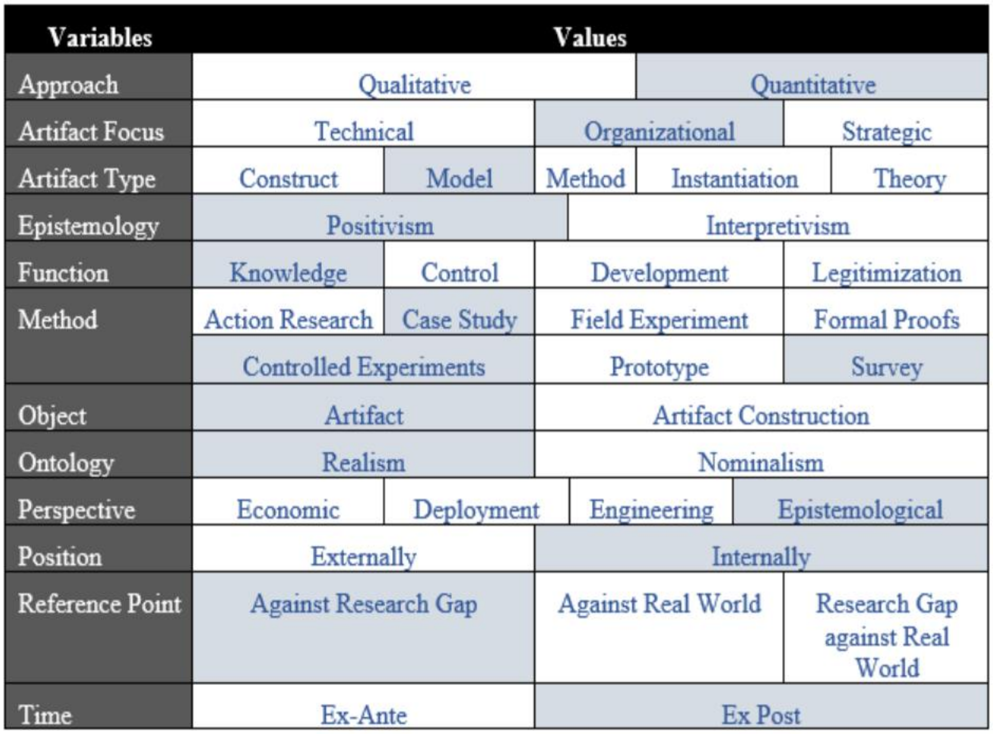
*would go to the financial team once the established system restore time exceeds the defined business limits for acceptable financial loss. Consequently, consideration can be made to reconcile financial and technical details to eliminate possible conflicts.*

*If implemented correctly in an organizational recovery planning process, the artifact appears to have features that will make collaboration efforts between the Information Technology Department and the Business Process office more productive and agreeable. The recovery objectives produced or validated by this process have a strong dependency on the system's previous record of performance. This relationship verifies that the recovery objectives are a better reflection of how the organization is likely to perform in a real incident.*

*For this reason, adjustments made to operational activities related to recovery are likely to be good for incident recovery preparation. I believe that acceptance of this process will be high among any organization's executives, as it eliminates the "guess work" that is often involved with generating recovery objectives. Also, I believe it represents a good start in the standardization of the process for establishing recovery objectives.*

## 6.5. Evaluation Summary

The variables relevant for the evaluation and their respective values are summarized and presented in figure 9. The shaded boxes are the selected values for each variable as applied in the evaluation of the artifact.



| Variables | Values | | | | |
|---|---|---|---|---|---|
| Approach | Qualitative | Quantitative | | | |
| Artifact Focus | Technical | Organizational | Strategic | | |
| Artifact Type | Construct | Model | Method | Instantiation | Theory |
| Epistemology | Positivism | Interpretivism | | | |
| Function | Knowledge | Control | Development | Legitimization | |
| Method | Action Research | Case Study | Field Experiment | Formal Proofs | |
| | Controlled Experiments | Prototype | Survey | | |
| Object | Artifact | Artifact Construction | | | |
| Ontology | Realism | Nominalism | | | |
| Perspective | Economic | Deployment | Engineering | Epistemological | |
| Position | Externally | Internally | | | |
| Reference Point | Against Research Gap | Against Real World | Research Gap against Real World | | |
| Time | Ex-Ante | Ex Post | | | |

Figure 9. Variables and values. Evaluation of DSR artifacts (Cleven et al., 2009)

## 6.6. Discussion

To address the problem of normalizing and standardizing the process of selecting recovery objectives as identified in the research problem, a decision model was proposed to provide guidance and standardize the process. The artifact was evaluated in an illustrative scenario where it was applied to a synthetic environment to demonstrate its utility and efficacy. The results of the evaluation were as expected. The values realized for the RTO and RPO were verifiably within the organization's tolerable limits and their relationship with other metrics involved in the overall recovery planning were clearly established.

The scenario presented a cyber incident that was announced by the organization at 12:00pm. The RPO was calculated at 4 hours, which initially placed the recovery target time at 8:00 am. Given that the RPO is only a goal, this indicated that the organization, with the availability of reliable recovery data, could have recovered their systems to a restore point later than 8:00am but not any earlier. Furthermore, based on the reporting requirements in NERC (2019) which placed the “time of discovery” at the highest priority, it would be advisable for the organization to select an earlier restore point. In this case, the organization would not be said to have met their recovery point objective. This is due to the time lag between when the incident was discovered and when it was acknowledged and reported.

Organizations usually conduct internal investigations to validate the incident details, gather all relevant information, and deem the incident reportable. In this scenario, with a shorter time lag between incident discovery and incident acknowledgement the organization would have met its recovery point objective.

In selecting the upper and low limits for the RTO range, using a Linear or Sequential restoration process where each sub-system is restored only after the previous one in the sequence has been completed, resulted in a longer total restoration time. In the given scenario, this total time exceeded the MTD, and would have prompted a revisit of the overall recovery and risk assessment process. When the Staggered recovery approach was used, and recovery activities on different subsystems can begin simultaneously, a shorter recovery time was recorded. This demonstrated that moving from the Linear approach to the Staggered approach can decrease the total recovery time, and therefore, where applicable, this might be a strategy to reduce the total recovery time. However, due to requirements such as separation of duties, or budget constraints in smaller organizations, resources or flexibility required to facilitate a Staggered approach might be limited or unavailable.

# CHAPTER 7
# CONCLUSION

Organizations benefit greatly from planning ahead for cyber incidents. In some cases, such planning can save the organization itself from a total collapse following a disaster. After evaluating the artifact produced in this research to answer the research question, it is evident that developing recovery objectives around an organization's technical and operational capabilities reduces the risk posed by unrealistic and non-feasible recovery goals. In this research, the objective was to find a way that the popular and widely accepted recovery metrics (RTO and RPO) can be established within an organization's tolerable limits and capabilities. Results from the survey showed that many organizations still prefer to use these metrics over others to test for cyber incident recovery readiness. These results further underscore the need to align these objectives to an organization's specific circumstances.

In establishing the RTO, two different requirements had to be satisfied. The first was to ensure that the RTO is equal to or larger than the time required to recover all systems ($RTO_1$). The second was to ensure that the RTO is less than or equal to a value ($RTO_2$) which is less than the tolerable limit (MTD) by a margin equal to or greater than the average margin of failure. For the RTO, the boundaries of the "safe" range were defined as $RTO_1$ and $RTO_2$. The "distance" between these two variables became the range within which the RTO can be safely established, making it easier to logically argue against setting the RTO outside this range. For the RPO, using the history of consecutive failures to justify the expansion of the value of the backup cadence or frequency showed that if the organization fared according to its history during a severe event, the expectations set by the value of the RPO will be within reason.

From the survey also, it was learned that majority of organizations have a formal declaration process for acknowledging cyber incidents. This declaration usually contains a recognition time upon which the recovery metrics are based. This time differs however from the acknowledgement time denoted by *tA* in the decision model. *tA* is the time of acknowledgement which is usually reported as part of the declaration.  It was also found that regardless of what "incident timing" was adopted, the relationship with the RPO remained the same. This means that the Actual Recovery Target Time would remain the same as the RPO unless the recovery point defined by the RPO was later than that defined by the company's preferred incident timing, in which case the Actual Recovery Target Time is a time earlier than the priority time for the incident, reduced by one hour to compensate for any margin of error.

## 7.1. Limitations and Challenges

In the course of the research, from the identification and validation of the problem to the design and evaluation of the proposed solution, several limitations and challenges were encountered. The most profound of these was the lack of availability of specific details from actual real-world incidents. Data from an incident such as whether drills were being conducted, what the results of those drills were, backup schedules and failure rates, selected recovery objectives, and BIA details are not readily available publicly due to privacy, legal, and in some cases, regulatory concerns. Another major challenge was the length of time it would take to completely assess the full impact of implementing the artifact. Assumptions, as detailed in sub-section 1.5, had to be made in order to predict the outcome.

## 7.2.Contributions

The findings of this research can be used to improve assessments of an organization's recovery preparation, particularly the feasibility of its recovery metrics. Attention can be drawn to other factors that contribute to recovery metrics in general, especially those that have little or no dependency on the IT department, such as the MTD. This can be especially useful in audits and other circumstances where regulatory oversight is necessary. As shown in the model, the meeting of, or failure to meet certain conditions can trigger or influence the employment of resources to improve some key components of a backup operation, thereby contributing to the overall cyber risk management process. Other possible uses of the decision model include a demonstration of due diligence and objectivity in internal self-assessment.

## 7.3. Future Research Direction

Future research efforts under this topic may seek to explore the relationship between the RTO and RPO as both are a reference to a point in time. Decisions on whether the very meaning of the RPO should be redefined as a function of the RTO as the "time" factor affects both increasingly, depending on the organization's business operations. Specifically, research efforts to further this study can aim to understand the following:

### 7.3.1. Related to the Decision Model

- How the model can be applied to fit an organization's specific circumstances such as time of high activity vs time of low or no activity to optimize targeted recovery

- What the tolerable limits could be for data loss expectancy and how to make such determination with reference to quantity of data as opposed to time
- Opportunities for automation and further customization of the decision model to fit specific environments
- How to determine the amount of data to be considered from system performance history
- Integration of this decision model into performance management and other capability management programs.

### 7.3.2. General System and Data Recovery

- The reasons why organizations might use a linear recovery approach instead of a staggered one
- The legal and regulatory environment of cybersecurity with specific focus on recovery requirements and related organizational responsibilities
- Compression algorithms used in backup technologies and their relationship with the causes and likelihood of backup restoration failure
- A deeper dive into the cause of backup failures such as Hardware failure, software corruption, and user error.

# REFERENCES

Alhazmi O. H. (2015). Computer-Aided Disaster Recovery Planning Tools. *International Journal of Computer Science and Security (IJCSS), 9*(3)

Arul, S., Modi, S., Bardallo, J., Codina, R., Jaeger, B., Keogh, C. C., … Lumpe, S. (2017). Improving Metrics in Cyber Resiliency. *Cloud Security Allliance* , 5–15. Retrieved from https://cloudsecurityalliance. org/download/improving-metrics-in-cyber-resiliency

Atiku, M., Garba, A. A., Bade, A. M. (2021). A Brief Analysis on the Existing Disaster Recovery Phases and Activities Plans. *International Journal of Software and Hardware Research in Engineering (IJSHRE), ISSN-2347-4890, 9*(2) pp. 55-64.

Baham C., Calderon A., Hirschheim R. ( 2017). Applying a Layered Framework to Disaster Recovery. *Communications of the Association of Information Systems, AIS* pp. 40, DOI: 10.17705/1CAIS.04012

Bodeau, D. J., Graubart, R. D., McQuaid, R. M., & Woodill, J. (2018). Cyber resiliency metrics, measures of effectiveness, and scoring: enabling systems engineers and program managers to select the most useful assessment methods. *(MTR180314)*. Bedford, MA: MITRE. Retrieved from https://www.mitre.org/

Cabrera, J. S., Luceno Reyes, A. R., Lasco, C. A. Multicriteria Decision Analysis on Information Security Policy: A Prioritization Approach. *Advances in Technology Innovation, 6*(1), pp. 1-7, January 2021. DOI: https://doi.org/10.46604/aiti.2021.5476

Carias, J. F., Labaka, L., Sarriegi, J. M., Tapia, A., Herantes, J. (2019). The Dynamics of Cyber Resilience Management. *CoRe Paper – T1 – Analytical Modeling and Simulation. Proceedings of the 16th ISCRAM Conference. Valencia, Spain. May 2019*

Chow, K., Deshpande U., Seshadri S., Liu L. (2021). SRA: Smart Recovery Advisor for Cyber Attacks. *2021 SIGMOD/PODS Conference*

Cleven A., Gubler P., Huner K. M. (2009). Design Alternatives for the evaluation of design science research artifacts. *Conference: Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology (DESRIST)*

Gedam, M. N., & Meshram, B. B.,  (2019). Vulnerabilities & Attacks in SRS for Object-Oriented Software. *World Congress on Engineering and Computer Science 2019 San Francisco, USA.*

Gomes, J. F., Ahokangas, P., & Owusu, K. A. (2016). Business modeling facilitated cyber preparedness. *International Journal of Business & Cyber Security (IJBCS)*, *1*(1), 1–10.

Goodwin P. (2021). The State of Data Protection and Disaster Recovery Readiness: 2021. *IDC #US47606921, April 2021*

Goud, D. (2019). Organizational Resilience Approaches to Cyber Security. *International Journal of Smart Education and Urban Society (IJSEUS)*, *9*(4), 53-62. DOI: 10.4018/978-1-5225-8897-9.ch057

International Standards Organization (2011). Guidelines for information and communication technology readiness for business continuity. *ISO/IEC 27031:2011*

Kawaguchi H. (2013). Study on the Gap Measures between Recovery Time Objective and Current Recovery Time in Business Continuity Management. *Nagoya Institute of Technology, Department of Social Engineering.*

Koulopoulos, T. (2017, May 11). 60 percent of companies fail in 6 months because of this (it's not what you think). *Inc. This Morning. Retrieved from https://www.inc.com/*

Luo J., Tang Q., Sun S., Li C., Zheng Y., Zhang M. (2020). The Security-Oriented Assessment Framework for Perception Layer of Electric Internet of Things. *Communications, Signal Processing, and Systems. CSPS 2020, Lecture Notes in Electrical Engineering, 654, Springer, Singapore 2021*. https://doi.org/10.1007/978-981-15-8411-4_177

Meilani D., Arief I., Habibitullah M. (2019). Designing Disaster Recovery Plan of Data System for University. *ICE&ICIE, IOP Conf. Series: Materials Science and Engineering 697  012028.* doi:10.1088/1757-899X/697/1/012028

Mendonca, J., Lima, R., Andrade, E., Araujo, J., Kim, D. S. (2020). Multiple-criteria Evaluation of Disaster Recovery Strategies Based on Stochastic Models. *16th International Conference on the Design of Reliable Communication Networks (DRCN).*

National Institute of Standards and Technology (2021). Contingency Planning Guide for Federal Information Systems (Rev. ed.). Department of Commerce, Washington, D.C. *NIST Special Publication 800-34 Rev. 1.* https://doi.org/10.6028/NIST.SP.800-34-r1

National Institute of Standards and Technology (2011). Managing Information Risk – Organization, Mission and Information System View. *NIST Special Publication 800-39*

Nejedlova D., Podaras A. (2017). Business Continuity – Risk Management VBA Software Tool (Version 1.0) – (BC-RM-V1.0). *Multiedu, Czech Republic*

North American Electric Reliability Corporation (2019). Cyber Security – Incident Reporting and Response Planning. *Implementation Guide for CIP-008-6.*

Onwubiko, C. (2020). *Focusing on the Recovery Aspects of Cyber Resilience*. Artificial Intelligence, Blockchain & Cyber Security Research Series, London, UK.

Peffers K., Rothenberger M., Tuunanen T., Vaezi R. (2012). Design Science Research Evaluation. *Design Science Research in Information Systems. Advances in Theory and Practice*. (398 – 410) DOI: 10.1007/978-3-642-29863-9_29.

Peffers K., Tuunanen T., Gengler C. E., Rossi M., Hui W., Virtanen V., Bragge J. (2020). *The* Design Science Research Process: A Model for Producing and Presenting Information Systems Research. *Proceedings Design Research Information Systems and Technology DESRIST'06.* 24.

Podaras A., Klara A., Jiri M. (2016). Information Management Tools for Implementing an Effective Enterprise Business Continuity Strategy. *E+M Ekonomie a Management, 19*, pp. 165-182, DOI: 10.15240/tul/001/2016-1-012

Podaras A., Moirogiorgou K, Zervakis M. (2021). Regression-Based Recovery Time Predictions in Business Continuity Management: A Public College Case Study. *IGI Global.* DOI: 10.4018/978-1-7998-4978-0.ch020

Podofillini, L., Wolfgang, K., Bruno, S. & Bozidar, S., (2015). IT contingency Planning for cyber disasters. Podofillini, L., Wolfgang, K., Bruno, S. & Bozidar, S., (Eds.), *European Safety and reliability of complex engineered systems* (pp. 221-227), Boca Raton: CRC Press.

Rabbani, M., Soufi, H. R., Torabi, S. A. (2016). Developing a two-step fuzzy cost-benefit analysis for strategies to continuity management and disaster recovery. *Safety and science 85*, 9-22

Romanosky S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2*(2), 2016, 121–135 doi: 10.1093/cybsec/tyw001

Ruddin, I., Santoso, H., Indrajit, R. E., Dazki, E. (2021). *Contingency Planning in IT Risk Audit on Music Digital Recording Company. Journal Of Music Science and Technology Industry (JOMSTI), e-ISSN. 2622-8211, 4*(2) 2021.

Russell D., Buffington J. (2021). How the last year has affected IT, Digital Transformation, and data protection strategy in ways NEVER seen before. *Veeam, Data Protection Report, 2021.*

Saaty R. W. (1987). The Analytical Hierarchy Process – What it is and how it is used. *Mat/d Modelling, Vol. 9, No.* 3-5, pp. 161-176, 1987

Sahebjamnia, N., Torabi, A., Mansouri, A., Salehi, N. (2011). A New Multi-Objective Scenario-Based Robust Stochastic Programming for Recovery Planning Problem. *Production and Operations Management Society (POMS) 23rd Annual Conference.*

Samimi A. (2020). Risk Management in Information Technology. *Progress in Chemical and Biochemical Research 2020, 3*(2), 130-134

Sicard K. (2019). The Need for Disaster Recovery and Incident Response: Understanding Disaster Recovery for Natural Disasters Versus Cyber-Attacks. *The Kennesaw Journal for Undergraduate Research. 6*(2). pp. 1-9.

Standardization Technical Committee of the National Information Security. Information security technology. Disaster recovery specifications for information systems. *(GB/T 20988-2007), 2007, 35.040, China National Standardization Administration Committee*

Steinberg, S. (2019, November 13). *Cyberattacks now cost companies $200,000 on average, putting many out of business.* Small Business Playbook. https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html

Suroso, A. I., Hamza, Sasongko H. An Early Warning System in the Drinking Water System. *International Conference on Sustainable Management and Innovation (ICoSMI), EAI, September 2021.* DOI: 10.4108/eai.14-9-2020.2304505

Taarup-Esbensen, J. (2020). The Business Impact Analysis. *Københavns Professionshøjskole* (pp. 1-20).

Tariq, M. I., Ahmed, S., Memon, N. A., Tayyaba, S., Ashraf, M. W., Nazir, M., Balas, V. E., Balas M. M. (2020). Prioritization of Information Security Controls through Fuzzy AHP for Cloud Computing Networks and Wireless Sensor Networks. *Sensors. September 2020, 20(5), 1310.* https://doi.org/10.3390/s20051310

Thomas, J. E., & Galligher, G. C. (2018). Improving backup system evaluations in information security risk assessments to combat ransomware. *Computer and Information Science, 11*(1), 14-25. https://doi.org/10.5539/cis.v11n1p14

Venable, J. R., Baskerville, R., Pries-Heje, J. (2012). A Comprehensive Framework for Evaluation in Design Science Research. *Design Science Research in Information Systems. Advances in Theory and Practice, May 2012.* (pp 423 – 438), Lecture Notes in Computer Science, vol 7286. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-29863-9_31

Wang G., Zhang L., Xu W. (2017). What Can We Learn from Four Years of Data Center Hardware Failures? *47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2017,* pp. 25-36, doi: 10.1109/DSN.2017.26.

Wieringa, R. J. (2014). Design Science Methodology for Information Systems and Software Engineering. *Springer*

Xu, S., Qian, Y. (2015). Quantitative study of reliable communication infrastructure in smart grid NAN. *11th International Conference on the Design of Reliable Communication Networks (DRCN) 2015*, pp. 93-94, doi: 10.1109/DRCN.2015.7148994

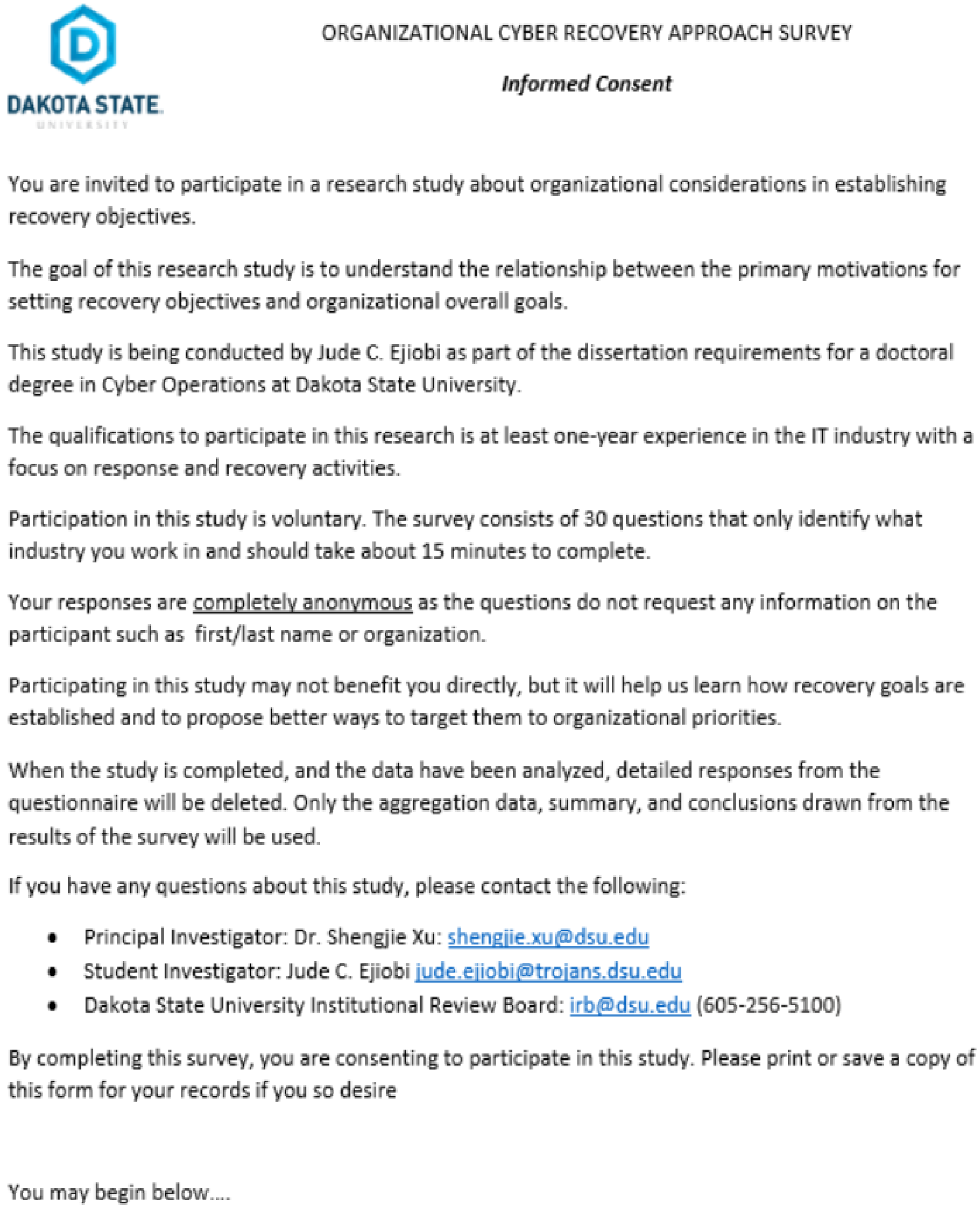
Xu, S., Qian, Y., Hu, R. Q. (2018). Reliable and resilient access network design for advanced metering infrastructures in smart grid. *IET Smart Grid, 1*(1), 24-30

Xu, S., Qian, Y., and Hu, R. Q. (2017). "A Study on Communication Network Reliability for Advanced Metering Infrastructure in Smart Grid," *IEEE Cyber Science and Technology Congress (CyberSciTech),* Orlando, FL, USA, November 6-10

Xu, S., Qian, Y., and Hu, R. Q. (2015). "On Reliability of Smart Grid Neighborhood Area Networks," *IEEE Access,* vol.3, pp.2352-2365

Zhu T., Xie Y., Song Y., Zhang W., Zhang K., Gao F. (2017). IT Disaster Tolerance and Application Classification for Data Centers. *Procedia Computer Science, 107, pp. 341-346, ISSN1877-0509.* DOI: 10.1016/j.procs.2017.03.115

# APPENDIX A: INFORMED CONSENT



DAKOTA STATE UNIVERSITY

ORGANIZATIONAL CYBER RECOVERY APPROACH SURVEY

***Informed Consent***

You are invited to participate in a research study about organizational considerations in establishing recovery objectives.

The goal of this research study is to understand the relationship between the primary motivations for setting recovery objectives and organizational overall goals.

This study is being conducted by Jude C. Ejiobi as part of the dissertation requirements for a doctoral degree in Cyber Operations at Dakota State University.

The qualifications to participate in this research is at least one-year experience in the IT industry with a focus on response and recovery activities.

Participation in this study is voluntary. The survey consists of 30 questions that only identify what industry you work in and should take about 15 minutes to complete.

Your responses are completely anonymous as the questions do not request any information on the participant such as first/last name or organization.

Participating in this study may not benefit you directly, but it will help us learn how recovery goals are established and to propose better ways to target them to organizational priorities.

When the study is completed, and the data have been analyzed, detailed responses from the questionnaire will be deleted. Only the aggregation data, summary, and conclusions drawn from the results of the survey will be used.

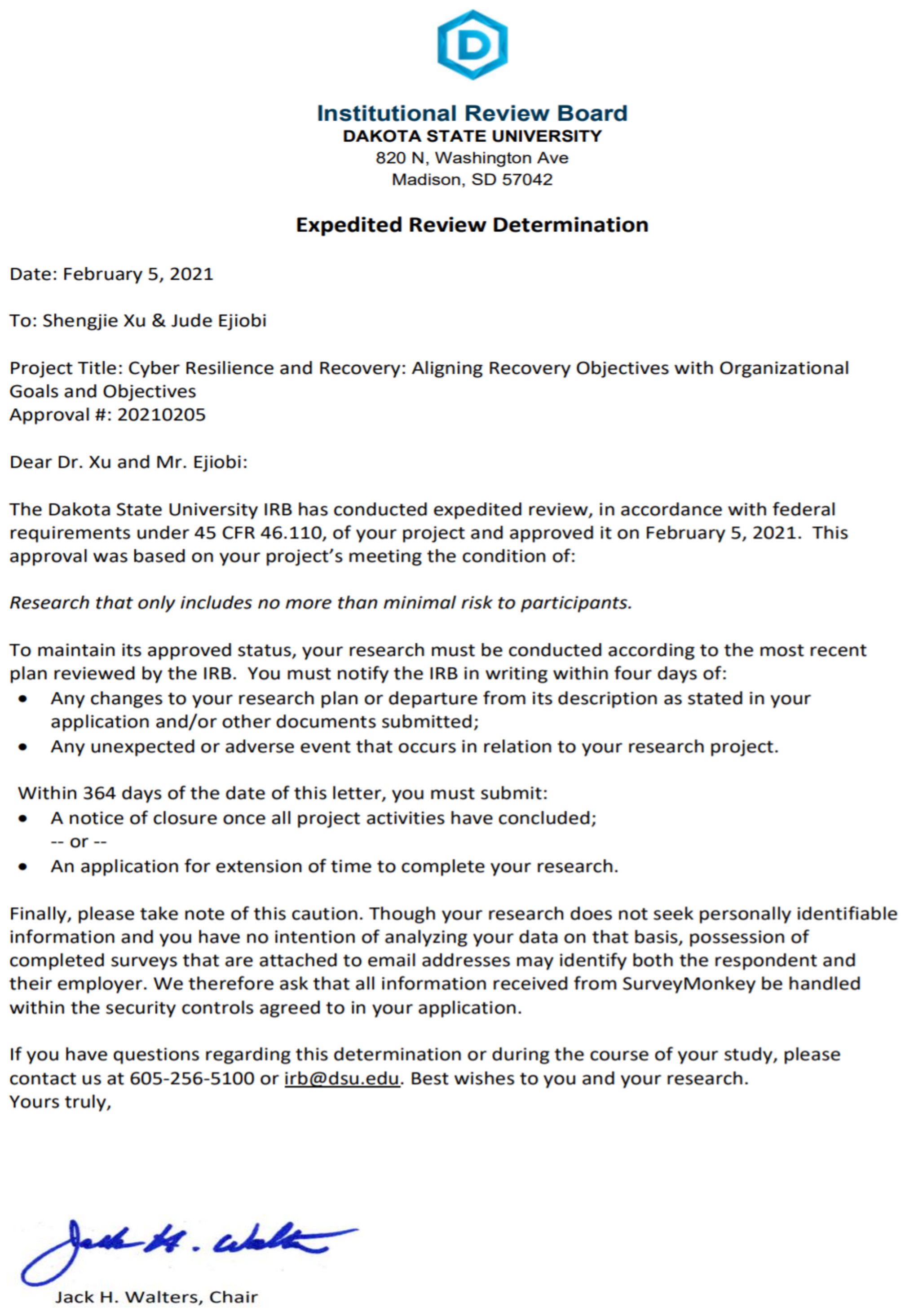
If you have any questions about this study, please contact the following:

- Principal Investigator: Dr. Shengjie Xu: shengjie.xu@dsu.edu
- Student Investigator: Jude C. Ejiobi jude.ejiobi@trojans.dsu.edu
- Dakota State University Institutional Review Board: irb@dsu.edu (605-256-5100)

By completing this survey, you are consenting to participate in this study. Please print or save a copy of this form for your records if you so desire

You may begin below….

# APPENDIX B: IRB APPROVAL



**Institutional Review Board**
**DAKOTA STATE UNIVERSITY**
820 N, Washington Ave
Madison, SD 57042

**Expedited Review Determination**

Date: February 5, 2021

To: Shengjie Xu & Jude Ejiobi

Project Title: Cyber Resilience and Recovery: Aligning Recovery Objectives with Organizational Goals and Objectives
Approval #: 20210205

Dear Dr. Xu and Mr. Ejiobi:

The Dakota State University IRB has conducted expedited review, in accordance with federal requirements under 45 CFR 46.110, of your project and approved it on February 5, 2021. This approval was based on your project's meeting the condition of:

*Research that only includes no more than minimal risk to participants.*

To maintain its approved status, your research must be conducted according to the most recent plan reviewed by the IRB. You must notify the IRB in writing within four days of:

- Any changes to your research plan or departure from its description as stated in your application and/or other documents submitted;
- Any unexpected or adverse event that occurs in relation to your research project.

Within 364 days of the date of this letter, you must submit:

- A notice of closure once all project activities have concluded;
  -- or --
- An application for extension of time to complete your research.

Finally, please take note of this caution. Though your research does not seek personally identifiable information and you have no intention of analyzing your data on that basis, possession of completed surveys that are attached to email addresses may identify both the respondent and their employer. We therefore ask that all information received from SurveyMonkey be handled within the security controls agreed to in your application.

If you have questions regarding this determination or during the course of your study, please contact us at 605-256-5100 or irb@dsu.edu. Best wishes to you and your research.
Yours truly,

Jack H. Walters, Chair

# APPENDIX C: SURVEY QUESTIONS

The following questions were presented to the survey participants:

## 1. Multiple Choice

1. Does your company conduct recovery drills?
    a. Yes
    b. No
2. If the answer to question 1 is "Yes," how often on average are the drills conducted?
    a. My organization does not conduct recovery drills
    b. Monthly (or more)
    c. Quarterly
    d. Biannually (twice a year)
    e. Annually (once a year)
    f. Biennially (once every two years)
3. If the answer to question 1 is "Yes," how often do you meet or exceed the goals set for recovery?
    a. N/A
    b. Always
    c. Most of the time
    d. Half the time
    e. Seldom
    f. Never
4. Does your company conduct separate recovery drills for natural disasters and man-made incidents (i.e. cyber incidents)?
    a. N/A
    b. Separate
    c. Together/Same
5. What Recovery Metrics do you use to measure success and/or failure, and test your recovery capabilities?
    a. N/A
    b. Traditional (RTO/RPO)
    c. Other
6. What industry would you consider your organization?
    a. Finance
    b. Healthcare
    c. Public Sector (Government)
    d. Energy/Utilities
    e. Retail
    f. Technology
    g. Entertainment
    h. Education

    i. Manufacturing
    j. Other

7. Is your company subject to any regulatory oversight?
    a. Yes
    b. No
8. If the answer to Question 7 is “Yes,” does the regulatory body have any requirements for recovery expectations?
    a. Yes, strict.
    b. Yes, relaxed.
    c. My organization is not subject to regulatory oversight
9. Which of the following will a successful cyber-attack on your organization have the most impact on?
    a. Confidentiality (exposure of sensitive information)
    b. Integrity (destruction of data)
    c. Availability (denial of service)
    d. Other
10. Which if the following variables are considered in the recovery planning?
    a. Backup Cadence (frequency with which backups are taken)
    b. MTD (Maximum Tolerable Downtime)
    c. Other
    d. Other (please specify)
11. Which of the following best describes your recovery process?
    a. None of the above
    b. Alternate site/environment running concurrently (Hot/Cold/Warm Site)
    c. Segmented, Tiered or Sequential recovery (storage-> data-> compute-> network-> applications)
12. With regards to time of recovery, how do you best describe the relationship between the components or layers of your IT environment?
    a. Sequential (once component or layer recovered after the other)
    b. Staggered and overlapping (recovery of different components can start concurrently regardless of dependency)
    c. Other (please specify)
13. If recovery of systems is layered, are there recovery objectives/metrics established separately for each layer, application or system?
    a. Yes
    b. No
    c. N/A
14. On a scale of 1-5 (1=Lowest, 5=Highest) how much does “time of failure or breach” matter with regards to recovery objectives?
    a. 1
    b. 2
    c. 3
    d. 4
    e. 5
15. On a scale of 1-5 (1=Lowest, 5=Highest) how important is the “time of discovery” of a breach or failure with regards to recovery objectives?

a. 1
b. 2
c. 3
d. 4
e. 5

16. What is your organization size?
    a. <100
    b. 100-500
    c. 500-1000
    d. 1000-5000
    e. >5000
17. Does your organization consider recovery objectives in data protection technology budgetary decisions?
    a. Yes
    b. No
18. Do you have recovery objectives for each layer/subsystem (i.e., Database, Network, Applications), or a general set of objectives?
    a. Separate
    b. General
19. What percentage of your IT budget is related to Business Continuity and Recovery?
    a. >5%
    b. 5%-10%
    c. 10%-15%
    d. 15%-20%
    e. >20%
20. Does your company have a different office or administration for Business Continuity or is it managed by IT?
    a. Different Office
    b. Managed by IT
21. What does your organization recognize as failure/outage?
    a. Partial outage (outage of any of the systems i.e., database, applications, files, storage)
    b. Full outage of all systems
    c. Exposure of confidential data (even with all systems fully functional)
    d. Compromise of data/services (even with all systems fully functional)
22. Which of the following does your organization recognize for the purpose of recovery objectives?
    a. Time of discovery
    b. Time of impact
    c. Time of breach
    d. None of the above
23. Does your organization have an official declaration of disaster and start of the “recovery” clock?
    a. Yes
    b. No

24. Does your organization distinguish between “time of breach” (if known), “time of discovery,” and “time of impact” if there is significant lapse of time between them for recovery metrics purposes?
    a. Yes
    b. No
25. On a scale of 1 – 5 how easy or hard is it to implement company-wide administrative (non-technical) information security controls that affect the entire organization (1 – easiest, 5 = Hardest)?
    a. 1
    b. 2
    c. 3
    d. 4
    e. 5

## 2. Short Response

1. Briefly describe what the consequences of a successful cyber-attack on your organization would be.
2. How are the variables of the recovery objectives derived/modified? (i.e., RTO, RPO)?
3. If the answer to question 1 in the Quantitative Inquiry section was “Yes,” (meaning that you do conduct recovery drills) what kind of drills do you conduct? Please provide a brief description.
4. How is official time of failure acknowledged? Is there an official declaration of disaster or is system failure acknowledged whenever your team discovers that certain services or systems are no longer functioning as expected?
5. Aside from regulatory requirements (if applicable) what are your organization’s other motivations for establishing recovery objectives?

# APPENDIX D: GLOSSARY OF ABBREVIATIONS

AR – Actual Recovery Target Point

BIA – Business Impact Analysis

CIA – Confidentiality, Integrity, Availability

CDP – Continuous Data Protection

CRT – Current Recovery Time

DRP – Disaster Recovery Planning

DSR – Design Science Research

ETIF – Elapsed Time to Identify Failure

ETIT – Elapsed Time to Identify Threat

IRB – Institutional Review Board

IT – Information Technology

MAO – Maximum Allowable Outage

MoE – Measure of Effectiveness

MoP – Measure of Performance

MTD – Maximum Tolerable Downtime

MTPD – Maximum Tolerable Period of Disruption

NERC – North American Energy Reliability Commission

RPO – Recovery Point Objective

RTE – Recovery Time Effort

RTO – Recovery Time Objective

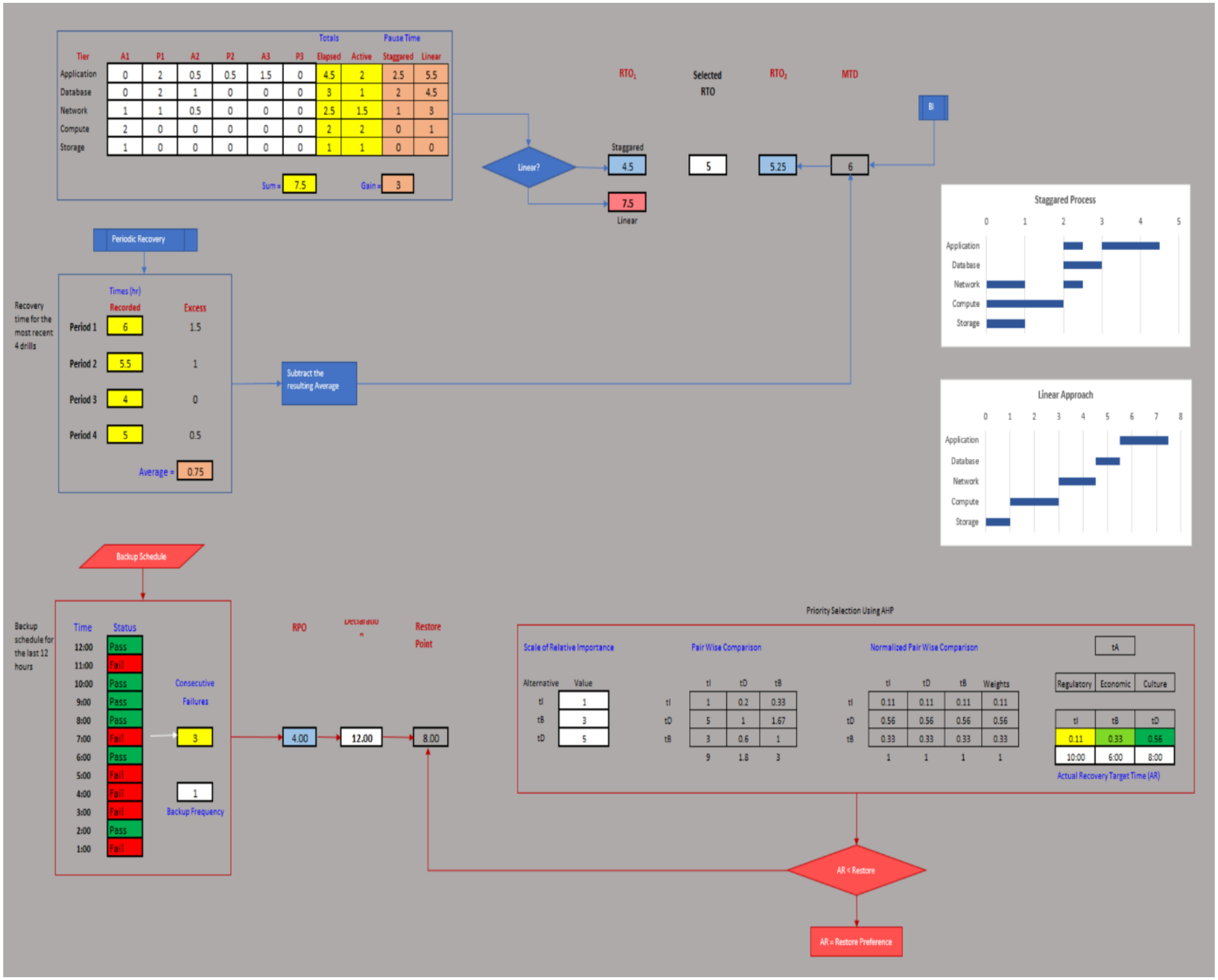
tA – Time of Acknowledgement

tD – Time of Discovery

tI – Time of Impact

tP – Timing Priority

# APPENDIX E: DEMONSTRATION EXHIBIT



|  |  |  |  |  |  |  | Totals |  | Pause Time |  |
|---|---|---|---|---|---|---|---|---|---|---|
| Tier | A1 | P1 | A2 | P2 | A3 | P3 | Elapsed | Active | Staggered | Linear |
| Application | 0 | 2 | 0.5 | 0.5 | 1.5 | 0 | 4.5 | 2 | 2.5 | 5.5 |
| Database | 0 | 2 | 1 | 0 | 0 | 0 | 3 | 1 | 2 | 4.5 |
| Network | 1 | 1 | 0.5 | 0 | 0 | 0 | 2.5 | 1.5 | 1 | 3 |
| Compute | 2 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 1 |
| Storage | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |

Sum = 7.5

Gain = 3

Recovery time for the most recent 4 drills

|  | Times (hr) |  |
|---|---|---|
|  | Recorded | Excess |
| Period 1 | 6 | 1.5 |
| Period 2 | 5.5 | 1 |
| Period 3 | 4 | 0 |
| Period 4 | 5 | 0.5 |

Average = 0.75

Backup schedule for the last 12 hours

| Time | Status |
|---|---|
| 12:00 | Pass |
| 11:00 | Fail |
| 10:00 | Pass |
| 9:00 | Pass |
| 8:00 | Pass |
| 7:00 | Fail |
| 6:00 | Pass |
| 5:00 | Fail |
| 4:00 | Fail |
| 3:00 | Fail |
| 2:00 | Pass |
| 1:00 | Fail |

Priority Selection Using AHP

Scale of Relative Importance

| Alternative | Value |
|---|---|
| tI | 1 |
| tB | 3 |
| tD | 5 |

Pair Wise Comparison

|  | tI | tD | tB |
|---|---|---|---|
| tI | 1 | 0.2 | 0.33 |
| tD | 5 | 1 | 1.67 |
| tB | 3 | 0.6 | 1 |
|  | 9 | 1.8 | 3 |

Normalized Pair Wise Comparison

|  | tI | tD | tB | Weights |
|---|---|---|---|---|
| tI | 0.11 | 0.11 | 0.11 | 0.11 |
| tD | 0.56 | 0.56 | 0.56 | 0.56 |
| tB | 0.33 | 0.33 | 0.33 | 0.33 |
|  | 1 | 1 | 1 | 1 |

tA

| Regulatory | Economic | Culture |
|---|---|---|

| tI | tB | tD |
|---|---|---|
| 0.11 | 0.33 | 0.56 |
| 10:00 | 6:00 | 8:00 |

Actual Recovery Target Time (AR)