

Towards A Methodology for Understanding Cyber Resilience Maturity in Organisations: A
Design Science Approach

BY

Yinhao Zheng

A thesis
submitted to the Victoria University of Wellington in
fulfilment of the requirements for the degree of
Master of Commerce

Te Herenga Waka — Victoria University of Wellington
(2023)

Towards A Methodology for Understanding Cyber Resilience Maturity in Organisations: A Design Science Approach

Abstract

As organisations pay increasing attention to cyber security due to the increasing threat of cyberattacks (Bendovschi, 2015; Lallie et al., 2021), the concept of cyber resilience is gradually becoming an important consideration (Bellini & Marrone, 2020). This study focuses on the challenge organisations face in cyber resilience management. It aims to design a methodology that assists them in understanding cyber resilience and positioning their maturity level by assessing implemented practices. The methodology – Cyber Resilience Maturity Assessment Methodology (CRMAM) – is designed following the Design Science Research approach proposed by Peffers et al. (2007) and evaluated by representatives from different industries. It analyses and interprets cyber resilience management from a high-level perspective, providing a quick assessment of the current maturity position and decision-making support of the future detailed framework adoption for organisations that do not have sufficient technology and financial support.

Table of Contents

Towards A Methodology for Understanding Cyber Resilience Maturity in Organisations: A Design Science Approach.....	1
Abstract	1
Acknowledgements.....	6
1. Introduction	8
2. Design Science Research as An Approach.....	8
3. Problem Identification	9
3.1. Tools or Solutions Provided in the Knowledge Base	12
3.2. Frameworks Identified in Cyber Resilience Area	15
4. Define the Objectives of the Solution.....	18
5. Designing, Building, and Evaluating	19
5.1. Design Cycle of Iteration 1	21
5.1.1. Designing CRMAM V.01	21
5.1.2. Building CRMAM V.01.....	29
5.1.3. Evaluating CRMAM V.01	37
5.2. Design Cycle of Iteration 2	39
5.2.1. Designing CRMAM V.02	39
5.2.1.1. Defining Governance	39
5.2.1.2. Defining Operations	40
5.2.1.3. Defining Controls	42
5.2.1.4. Defining Relationships of Categorisations	43
5.2.2. Building CRMAM V.02.....	44
5.2.3. Evaluating CRMAM V.02	47
5.3. Design Cycle of Iteration 3	49
5.3.1. Designing CRMAM V.03	49
5.3.2. Building CRMAM V.03.....	51
5.3.3. Evaluating CRMAM V.03	59
5.3.3.1. Essential for Design Objectives.	60
5.3.3.2. Nice-to-have for Future Work.	64
5.3.3.3. Good Idea but Out of Scope.....	65
5.4. Design Cycle of Iteration 4	67

5.4.1. Designing CRMAM v.04.....	67
5.4.2. Building CRMAM V.04.....	70
6. Communication.....	76
6.1. Contributions	76
6.1.1. Methodology	76
6.1.1.1. Target Audience.....	76
6.1.1.2. Framework	77
6.1.1.3. Supplementary Materials.....	81
6.1.1.4. Connections with DSR Studies	83
6.1.2. Methodology as Contribution	84
6.1.2.1. To Practice	84
6.1.2.2. To the Knowledge Base	86
6.2. Observations	87
6.2.1. Trends of Concepts in Cyber Resilience Management	87
6.2.2. Lack of Practices Related to Governance in three Functions.	88
6.2.3. Concerns of Governance in Organisations	89
6.2.4. Lack of Understanding of the Organisation's Maturity	90
7. Limitations.....	91
8. Future Work	92
9. Conclusion.....	94
Appendices.....	96
Appendix A	96
Appendix B	98
Appendix C	100
References.....	102

List of Tables

Table 1: Solution examples identified from the knowledge base.	12
Table 2: Identified framework details.	15
Table 3: Selection criteria for framework review.	22
Table 4: New selection criteria for framework review.	23
Table 5: The weighting matrix.	23
Table 6: Concept matrix for reviewed frameworks (baby-step).	26
Table 7: Markers and meanings for framework reviewing.	27
Table 8: Concept matrix for reviewed frameworks (adult-step).	28
Table 9: Modifications in the EDM domain.	52
Table 10: Feedback grouped by importance.	60
Table 11: Feedback that is essential for design objectives.	61
Table 12: Feedback that nice-to-have.	64
Table 13: Feedback that is a good idea but out of scope.	65
Table 14: Example of the colour system.	72
Table 15: Interviewee's attributes.	100

List of Figures

Figure 1: Relevance and rigor cycle of problem identification (Adopted by Hevner & Chatterjee (2010).	14
Figure 2: Design cycles of research (Adopted by Peffers et al., 2007).	20
Figure 3: Mind map for concepts and their core elements.	35
Figure 4: Screenshot of CRMAM V.01 (partially).....	36
Figure 5: Code example of each practice.	38
Figure 6: The relation maps for categorisation.	43
Figure 7: Screenshot of CRMAM V.02 (partially).....	46
Figure 8: Group by domains [Version 1].....	54
Figure 9: Group by categorisation [Version 2].	55
Figure 10: Group by lifecycle [Version 3].	56
Figure 11: Reference sheet for sub-categories (partially).	58
Figure 12: Redesigned relationship map.....	71
Figure 13: Graphical expression of CRMAM result.	73
Figure 14: Screenshot of CRMAM V.04 (partially).....	75
Figure 15: CRMAM final version – grouped by domains [Version 1] (partially).....	79
Figure 16: CRMAM grouped by categories [Version 2].	80
Figure 17: CRMAM grouped by lifecycle [Version 3].	81
Figure 18: Relationship map.	82
Figure 19: Reference sheet for sub-categories.	83
Figure 20: Comparison of practices by categories and functions.	88

Acknowledgements

I would like to thank my supervisor, Dr. Cathal Doyle, for teaching me throughout my postgraduate studies. Coincidentally, you are one of my supervisors from the first course I took for postgraduate to the last research project. Your time, effort, guidance, and insights into this research have made me a step closer to becoming a more mature academic. I remember your example of “Standing on the shoulders of giants” in the first lecture. For me, you are the “giant” that carried me through this achievement. Fortunately, you are “tall enough” to let me have the luck of seeing the world of “scholars”. More amazingly, your ever-positive personality has influenced me many times, teaching me to overcome anxiety, encouraging me to be brave and boosting my self-confidence. You have taught me more than just how to complete a study, an assignment, or a course, you have shaped me into a better version of myself. Thank you for putting up with my message after message, especially close to the due day (sorry, I know it is not very pleasant), you are the coolest teacher I have ever had! A simple paragraph is not enough to express all my gratitude, but I will always remember this time as the supervisor-student relationship.

I would also like to thank Dr. Ian Welch and Dr. Masood Mansoori, as my co-supervisors, for your generous support of my studies. You gave me confidence by participating in interviews when I was timid to face unfamiliar interviewees on my own, always responded to my emails promptly and provided detailed explanations and made valuable advice on how to make the study better. For all of this, I would like to thank you for your dedication and support.

Thank you to Paul McTaggart for your professional guidance and timely feedback. Your insightful and practice-oriented perspective has always kept this study on the right track and filtered the redundant distractions. I have to say that those small chats before the meeting at the beginning of the project really helped me to relax and dare to share my views.

A special thanks to my parents Chengzhao and Xiangping. Thank you for all the support and help you have given me. Without your encouragement and support, I may never have been brave enough to step out of my comfort zone and choose to study and live on the other side of the world. Not only have you given me the freedom to explore the world, but you have also given me a backup and “roof” over my head when facing the storms in my life.

Thanks to all my friends. Thanks, Alex, for providing me with proof-reading my thesis and helping me correct the verb tense. You never laughed at my English or my bad grammar, and you patiently read through my super-long draft and gave suggestions to improve my thesis. Thanks to Alexa for lending me Grammarly to check grammar and sharing your cat with me for “pet therapy”. Thanks all my friends for your company and the joy you brought.

I would like to thank Juno for the happiness, companionship and love you have brought me. Without your company and care, my life would have been full of break nights and junk food for the past two years. You always prepared delicious food and reminded me to eat, rest, and exercise regularly. You were always here whenever I needed you, to proof-reading my essays, consolidate my thoughts, and provide other assistance. You always listened patiently to the dramas and joys I encountered at school and work. Even though you sat next to me playing games every time I did my assignments, it helped enhance my concentration.

Finally, thanks to myself. If I had been told ten years ago that today I would be sitting in another country finishing my thesis, I would have thought it was a dream. Fortunately, with the help of my family, friends and teachers, this dream has become a reality. Thank you for your continued perseverance and hard work. Come rain or shine, you keep improving and becoming a better version of yourself.

Thanks to everyone who contributed and supported this study. Thank you to those who have helped me along the studying for improving my confidence and courage to face challenges. Thank you to the people who have given me a hard time (although I still hate you), these experiences have made me a stronger person.

1. Introduction

Improvements in technologies stimulate organisations to adopt new technologies to stay competitive. However, these adoptions also expose them to heightened risks in cyberspace. Exposed information and business activities attract attackers' attention and threaten organisations' ability to function (Andronache, 2021; Pupillo, 2018). Organisations try to defend against attacks and recover from incidents by adopting more technologies, but thoughtless adoption leads to higher technology dependency and exposure (Arora et al., 2004; Fielder et al., 2016). These cascading attacks not only cause serious financial losses to organisations but also create obstacles for organisations to maintain critical services and operational processes. Potential negative reputational impact and customer distrust can also cause pain to organisations.

Some academics suggest enhancing cyber resilience as a way to reduce losses and improve the ability to detect and defend against cyberattacks (Benz & Chatterjee, 2020; Linkov & Kott, 2018). The term "cyber resilience" has been widely discussed in studies (Carías et al., 2019; Hausken, 2020). The Financial Stability Board (FSB) defines cyber resilience as "The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents" (Financial Stability Board, 2018, p.9). Björck et al. (2015) examined cyber resilience from an organisational perspective and defined it as maintaining delivery even when adverse events happen.

This study collaborates with a cyber resilience organisation focussing on cyber resilience management in New Zealand organisations. We found that one of the main reasons for most organisations' cyber resilience failures is the lack of a comprehensive understanding of cyber resilience and an effective cyber resilience plan. To assist them in addressing this issue, we believe an efficient approach is needed for organisations building an understanding of cyber resilience and conducting maturity reviews. So we designed a methodology guided by Design Science Research (Hevner et al., 2004; Peffers et al., 2007), which we explain in the following section.

2. Design Science Research as An Approach

This study follows the design science research approach (DSR). DSR is known for focusing on

developing artefacts that can solve real-world problems (Nagle et al., 2020; Peffers et al., 2007). It identifies problems and provides solutions from the field of practice and the knowledge base (Iivari, 2015) based on balancing rigour and relevance (Gregor & Hevner, 2013). Some researchers (Nagle et al., 2020; Nunamaker et al., 2015) emphasise that the final research mile is completed when the researcher designs solutions that actually solve practitioners' problems in practice, which not only demonstrates the true impact of the research, also reduces barriers for practitioners in accessing and interpreting these DSR results. Here, DSR satisfies two goals of this research (Hevner et al., 2004; Hevner & Chatterjee, 2010): 1) Building artefacts to solve problems in the appropriate setting; 2) Contributing new knowledge to the IS knowledge base. This study follows the DSR process model proposed by Peffers et al. (2007) as it establishes a general framework for researchers to conduct effective DSR.

This process model consists of five steps (Peffers et al., 2007). 1. Problem Identification: we collaborated with practitioners to define problems of New Zealand organisations' cyber resilience management; 2. Define Objectives of a Solution: we defined the design objectives that the artefacts needed as a solution; 3. Design and build: we conducted four design iterations to design and refine artefacts to ensure their functionalities; 4. Demonstration and Evaluation: after completing each design and build phase, we demonstrated the artefacts to evaluators and gathered their feedback. The artefacts were iterated back and forth through these Design Cycles; 5. Communication: after all Design Cycles were finished, we communicated the components of artefacts and how to use them. The problem identification step is introduced in the next section.

3. Problem Identification

In recent years, organisations have realised the convenience of information technology. It plays an important role in business practices by offering abundant opportunities to operate from multinational companies with large servers to small businesses with just a few tablets. However, this has led to an increasing reliance on cloud-based technology for organisations. This reliance has also resulted in organisations becoming more vulnerable to cyber threats (Andronache, 2021; K. Huang & Pearson, 2019; Pupillo, 2018). These potential vulnerabilities offer a "tempting cake" that attracts the attention of cyber attackers. Recent research has shown that organisations worldwide have experienced a 31% increase in cyberattacks in 2021 compared to 2020 (Bissell et al., 2021). Therefore, the question of how to enjoy the dividends of technological advances while avoiding the pitfalls of

cyberattacks has become an important issue for organisations to address.

Thus, organisations worldwide employ many means to enhance prevention, detection, and response capabilities for cyber incidents. Adopted methods also aim to increase cyber resilience maturity, such as investing in cyber security software (e.g., firewalls, spam blockers), hiring qualified cyber security experts to fill the roles, or outsourcing cyber security maintenance with service providers. New Zealand organisations are no exception and put efforts into their cyber security. For example, the Reserve Bank of New Zealand introduced cyber resilience risk management guidelines for financial sectors experiencing the most cyberattacks (Reserve Bank of New Zealand, 2022). Another industry that has received a lot of attention – the healthcare industry – also developed cyber security response plans, such as the 2019 cyber security strategy (Fonseka, 2021).

Governments are also working with organisations to provide a range of policies to maintain cyber security environments. In America, former President Barack Obama issued a series of executive orders (e.g., Executive Order 13636, 2013) to address cyber threats by improving cyber infrastructure security (Linkov et al., 2013). The UK formulated and published the National Security Strategy in 2010 (Harrop & Matteson, 2013), which mainly identified 15 priority types of 4 major risks. Some countries in the Asia-Pacific, like Japan and Singapore, developed national cyber security strategy documents (Christine & Thinyane, 2020b). Australia is also learning from America to improve its cyber security plan (Joiner, 2017). And New Zealand's government not only supports the development and innovation of the local cyber security industry but also provides cyber security assistants to small and medium-sized organisations (SMEs) (Christine & Thinyane, 2020a, 2020b).

However, these seemingly well-established and rigorous responses have not successfully brought total security to organisations. Just five months after risk management guidelines were released, several financial institutions such as Kiwi Bank, ANZ, and the Inland Revenue experienced serious cyberattacks (Checkpoint, 2021). According to a survey released by Kordia's Aura Information Security in 2021 (Aura News, 2021), more than half (55%) of Kiwi businesses had been successfully targeted by a ransomware attack in the previous 12 months (Chiang, 2022). One of the root causes of this situation is that most organisations still lack a comprehensive understanding of cyber resilience and appreciation of their cyber resilience maturity. Some organisations mistakenly believe that a causal relationship exists between technical cyber security investment and reduced risk of

cyberattacks.

In fact, the increased complexity associated with continued investment in cyber security technology tools instead reduces an organisation's ability to respond effectively to cyber security threats (Shackleton, 2021). However, despite the significant increase in cyberattacks and cyber security spending, only a minority of executives claimed that their organisations were prepared to deal with the potential of cyberattacks (Shackleton, 2021). More seriously, "ignorance can be bliss" (Benz & Chatterjee, 2020, p.532). Some organisations' leaders who are overconfident in their preparedness and defensive capabilities believe that their security is above average, while their cyber resilience maturity may be exceptionally low. This misconception results in an inability to direct manage and monitor their cyber security risks.

This opinion is also reinforced by the organisation this study worked with. This organisation is a New Zealand-based SME who specialises in cyber resilience consultancy and technical support to organisations for almost 30 years. Through their practice in recent years, they found that most New Zealand organisations' understanding regarding cyber resilience is still at a very basic level. They believe that organisations do not have a comprehensive understanding of the overall cyber resilience maturity within their organisation, nor a reasonable assessment of their overall maturity status, therefore they lack the direct operations and technology investments and are aligned and prepared to respond to cyber incidents. This study was initiated to understand this problem by conducting a systematic review of the current knowledge base, to see if any applicable solutions have already been made available.

According to DSR (Hevner et al., 2004), after identifying a relevant problem in practice, IS researchers should look to the current knowledge base to understand the problem and relevant applicable knowledge. This step aims to look for available tools, theories, and frameworks to solve the problem, and assist in constructing a solution by reviewing previous research and reference disciplines (Hevner et al., 2004). Thus, we reviewed the existing knowledge base in the cyber resilience area to identify if the problem has been addressed or discussed. Based on the problems identified among practitioners, this study defined several keywords ("cyber resilien*" AND ("organisation*" OR "organization*" OR "compan*" OR "enterprise*")) to be used in the search for relevant studies. Web of Science (WoS) was selected as the database to search for these key terms as it is one of the most

authoritative and widely used research engine (Birkle et al., 2020).

Initially, we found 66 articles and promptly categorised them in a concept matrix (Webster & Watson, 2002) by following the methodology of Nagle et al. (2020). Then, after an initial analysis of the titles, abstracts, keywords, and content of these articles, we excluded 6 of the irrelevant results by browsing the article's content and analysed 60 articles in depth (you can find the literature review and concept matrix here: <https://osf.io/q7gpx/files/osfstorage/649bd3a03809110ca13c32fa>). During our review, we kept two goals in mind: 1) To check if academics or practitioners have proposed any solutions to the problem, and 2) To look for frameworks that could assist in understanding the problem and conceive of what components are required in possible solutions.

3.1. Tools or Solutions Provided in the Knowledge Base

We compared the solutions provided in the studies. Most studies provided solutions to assist organisations in improving maturity through one or several aspects of cyber resilience. We have grouped them according to contribution types of DSR artefacts (Gregor & Hevner, 2013; Hevner & Chatterjee, 2010) and selected a few representative artefacts as examples summarised in Table 1.

Table 1: Solution examples identified from the knowledge base.

Artefact	Examples	
	Author	Artefact Description
Approach	Estay (2021)	An approach for high-level cyber-resilience to zero-day vulnerabilities.
Framework	Carías, Borges, et al. (2020)	A framework with corresponding implementation orders for SMEs.
Measure	Khan & Estay (2015)	A future research agenda for supply chain cyber-resilience.
Method	Benz & Chatterjee (2020)	An SME cybersecurity evaluation tool (CET).
Model	Carías, Arrizabalaga, et al. (2020)	A cyber resilience progression model.
Procedure	Gafic et al. (2021)	A table-top cyber security exercise lecture procedure.
System	Onishchenko et al. (2022)	A data exchange protocol and an algorithm for detecting “dangerous” keywords in messages.

In addition, we noted that some studies were conducted in countries similar to New Zealand. Most of the organisations in their research environment are SMEs. We provided a detailed analysis of the tools used in these studies.

Wong et al. (2022) discussed the cyber security awareness of Malaysian SMEs and their cyber security practices and found that most respondents recognised the importance of improving cyber resilience, so adopted employee training as a critical first step in improving resilience. Unfortunately, the practices taken by interviewees were neither made available to the public nor the research tool they used, which means it is not easy for organisations and academics to review the practices of others and learn from them. van der Kleij & Leukfeldt (2020) integrated cyber resilience and human behaviour models, and after a pilot study of 60 SMEs in the Netherlands, proposed a cyber resilience framework that combined four resilience functions and three sources of behaviour, which nevertheless only focused on measuring the impact implementation of that framework had on the employees during testing. Thus, for our purposes the tool is not applicable.

Tam et al. (2021) discussed, through an Australian organisation lens, the improvement room for small businesses in terms of cyber resilience actions. They highlighted that copying cyber resilience solutions from large organisations is impractical due to differences in cyber security human resources and technical environment. But despite an in-depth understanding of the challenges and opportunities that SMEs face, they did not offer a clear solution to solve the problem. In contrast, the SMEs cyber security evaluation tool proposed by Benz & Chatterjee (2020) is arguably one of the most suitable tools. They filtered and simplified the criteria included in professional frameworks, resulting in 35 criteria that were most relevant to reducing the operational risk profile of SMEs. However, almost all evaluators were experts with extensive IT/IS experience, meaning they had less technical barriers. Organisations might be difficult to make accurate assessments in real-world environments without comparative data and specialised expertise.

Besides these frameworks proposed by academics, there are some other popular solutions among practitioners. Firstly, cyber exercises. Some governments see “cyber exercises” as a solution to cyber resilience by simulating different scenarios of cyber incidents to cultivate organisations’ ability to respond to real situations (NCSC, 2018; Ruefle et al., 2013). Several guidelines to support

organisations in conducting cyber exercises were introduced. In Europe, the EU Agency for Network and Information Security provides guidance for organisations (Catteddu & Hogben, 2009). The Finnish Cyber Exercise Organiser's Handbook lists the most important types and explains how to organise regular exercises (Gafic et al., 2022; Jensen, 2019). Secondly, cyber security regulations. Practitioners also are actively developing regulations to improve cyber security protection (Pernice, 2018; Reserve Bank of New Zealand, 2022). In the US, for example, one of the first major initiatives taken by the Department of Defense (DoD) in 2016 was the introduction of new cyber security standards (Ross et al., 2021).

Through the review of the knowledge base and practice, we found that organisations are caught in an expanding technology cycle (see Figure 1) regarding cyber resilience management. While adopting an increasing breadth of new technologies can help organisations temporarily deal with cyber threats, it does not solve the underlying problem. The high technology variation and dependence exacerbated by incomplete or improper adoption also create new potential risks. Although some organisations desire to improve understanding and conduct cyber resilience reviews, solutions from the knowledge base are unfortunately not reasonably available to them mainly because of the following two reasons.

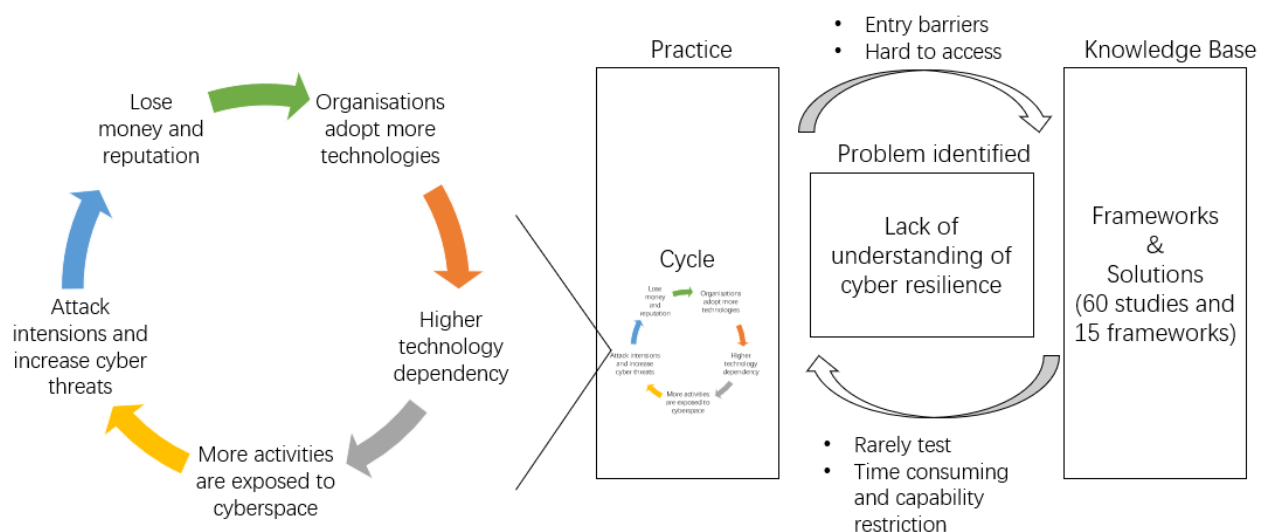


Figure 1: Relevance and rigor cycle of problem identification (Adopted by Hevner & Chatterjee (2010)).

Firstly, the limited resource of organisations (Benz & Chatterjee, 2020; Carías et al., 2021). Most organisations' primary goals in highly competitive environments are making profits and improving

competitiveness. The resources they can allocate to cyber resiliency management are insufficient, restricting their ability to utilise professional frameworks (Tam et al., 2021). Secondly, high entry barriers to these frameworks (Zhang et al., 2020). Designers provided as detailed and comprehensive support as possible for these well-designed frameworks to help users understand and use them accurately. The purpose of this thinking is good, but the overload of information also results in time-consuming and effort-consuming for users to familiarise and master them. Interestingly, while many solutions were proposed, only 13% of the reviewed articles tested their solutions. Most of them were tested through case studies or laboratory simulations. Those tested solutions are also difficult to access publicly. Due to these limitations, we believe a better solution to organisations' problems in the New Zealand environment is still needed.

3.2. Frameworks Identified in Cyber Resilience Area

In the first round of the literature review, we acknowledged the necessity of an appropriate solution, as existing solutions have limitations. To identify the new solution's essential components and clarify the objectives of the designed solution, we needed to gain insights from concepts and structures of other frameworks in the knowledge base. Therefore, we conducted a second literature review and captured 15 frameworks as shown in Table 2.

Table 2: Identified framework details.

Framework	Description	Reference
National Academy of Sciences (NAS) 4 phases	A four-phase approach (prepare, absorb, recover, and adapt) for resilience management to predict attacks in advance and plan to reduce their impact instead of waiting for an incident to occur and taking the loss afterwards.	The National Academy of Sciences (2012); Zemba et al. (2019)
Network-Centric Warfare (NCW) doctrine	The US Army's NCW doctrine suggests four domains (physical, information, cognitive and social) to enable resilience assessments in complex systems.	Collier et al. (2014); Paradis et al. (2005)

Cyber Resilience Matrix	A resilience matrix framework for assessing critical services in organisational systems and an updated version by adjusting the resilience matrix framework and drawing on metrics from several academics to customise the generic framework for the cyber security domain.	Linkov, Eisenberg, Bates, et al. (2013); Linkov, Eisenberg, Plourde, et al. (2013); Linkov & Kott (2018)
National Institute of Standards and Technology Cyber Security Framework (NIST CSF)	A framework created by a partnership of industry and government and is based on cyber security-related standards, guidelines and practices designed to help organisations identify and mitigate cyber risks in critical infrastructure.	Benz & Chatterjee (2020); NIST (2018)
Cyber Resilience Review (CRR)	An assessment tool for evaluating an organisation's operational resilience and level of cyber security practices	Caralli et al. (2007)
Cybersecurity Capability Maturity Model (C2M2)	A model that can allow organisations to evaluate their cyber security capabilities and optimise security investments.	Curtis et al. (2015); Muneer (2022)
Cyber Resiliency Engineering Framework (CREF)	A framework that systematically defines the cyber resiliency's objectives and lists techniques that can be applied to improve cyber resilience	Bodeau et al. (2012)
Cyber Resilience Progression Model (CRPM)	A progression model that describes the characteristics, attributes, and evolution of cyber resilience policies over time and provides a basic to mature guide for organisations to manage their cyber resilience.	Carías, Arrizabalaga, et al. (2020)
Cyber Resilience Self-Assessment Tool (CR-SAT)	A web-based tool modified from CRPM, focusing on SMEs and providing a self-assessment of cyber resilience maturity in various domains.	Carías et al. (2021)

CERT Resilience Management Model (V 1.2) (CERT-RMM)	A resilience management model that makes operational resilience a “repeatable, predictable, manageable, and improvable process” (Caralli et al., 2016, p.1165) through 12 interrelated aspects.	Caralli et al. (2016)
Managerial Cyber Resilience Framework (MCRF)	A framework that discusses three key contextual factors for cyber resilience implementation (infrastructure, industry, and ownership) and uses the cyber resilience lifecycle to summarise cyber resilience-related practices and identifies their impacts.	Annarelli et al. (2020)
Cybersecurity Risk Management (CSRM)	A risk management methodology incorporates the NIST methodology of risk assessment, risk mitigation, and monitoring/controls in a three-step process.	Katsumata et al. (2010)
Information Security Focus Area Maturity Model (ISFAMM)	A model that contains 13 key areas and four categories to aid organisations with designing information security programs, and establishing high-level guidelines.	Spruit & Roeling (2014); Spruit & Slot (2017)
Cybersecurity Maturity Assessment Framework (CMAF)	A framework that allows basic service operators and digital service providers to conduct self-assessments and perform gap analysis with a graphical representation of the results.	Drivas et al. (2020)
Australia Energy Sector Cyber Security Framework (AESCSF)	A set of cyber security guidelines is designed to support Australian energy infrastructure industry operators in reviewing, assessing, and improving their cyber security situation.	AEMO (2021)

These frameworks provided suggestions around cyber resilience from various perspectives, with some including detailed considerations around a particular area of cyber resilience, such as information security, and risk management. Some focus on discussing categories of resources

related to cyber resilience. Frameworks with different levels of expertise also have varying degrees of overlap in concept coverage. This might influence the organisation's adoption. Therefore, after gaining insight into these frameworks, we identified a series of design objectives that could avoid these problems, which are discussed in the next section.

4. Define the Objectives of the Solution

To assist organisations in solving the problem, the objective is to create a methodology that allows organisations to evaluate their cyber resilience maturity. To allow organisations to perform cyber resilience reviews and maturity assessments independently, the methodology should meet the following objectives:

Design objective 1: Have comprehensive coverage and precise definition of concepts.

Although the term “cyber resilience” is gradually being emphasised and used, there is still ambiguity in the practical application of the term, such as cyber security and information security. This interchange is not only presented in practitioners' applications but also mentioned in academic articles (Azmi et al., 2018; von Solms & von Solms, 2018). Therefore, the methodology should clearly define the concepts of cyber resilience. Similarly, reviewing the knowledge base shows that solutions are various regarding coverage and level of detail, which somewhat increases the difficulties for organisations to utilise them. This requires that our methodologies should establish comprehensive coverage to reduce misconceptions.

Design objective 2: Include the essential practices and detailed descriptions.

The methodology should include essential practices with detailed supplementary materials to provide organisations with a proper understanding. Meanwhile, it is necessary to note that the methodology should provide a concise version and not be overly complicated, as this can lead to higher learning and usage costs, which is difficult to use for organisations that are just beginning their cyber resilience management journey or have limited resources in cyber resilience (Carías, Borges, et al., 2020).

Design objective 3: Have corresponding references to map concepts across frameworks.

Some organisations that have started cyber resilience management may have adopted a set of frameworks that guide practices. In this case, interoperability of widely-used frameworks and designed artefacts can reduce duplication of effort (Azmi et al., 2018) and minimise overlap between reviews and practices. One means of facilitating interoperability is to make the methodology reflect the linkage from artefacts to those widely used frameworks. It allows organisations to map the same practices across frameworks and use these references to understand practices more accurately. For the methodology, this mapping also makes the practice more compelling.

Design objective 4: To be understandable, unambiguous, and applicable for experts and non-experts.

For most organisations, the staff assigned to review cyber resilience practices are typically those with expertise and responsibility for cyber security management. However, some organisations, especially small- and micro-organisations, have limited resources to face cyber threats, and lack sufficient staff dedicated to cyber security or cyber resiliency management (Furnell et al., 2017). For such organisations, it is necessary to improve the usability of the methodology and reduce the complexity and entry barriers. The language and structure used in the methodology should reflect this consideration.

Overall, the primary goal of this study is to create a methodology that meets these four design objectives, with the long-term goal as to assist New Zealand organisations in gaining a grasp of their cyber security plan and, to a more considerable extent, the New Zealand environment's cyber security and awareness of the importance of enhancing cyber resilience. The methodology will be developed to ensure it applies to different industries and organisations.

5. Designing, Building, and Evaluating

To design artefacts that meet the design objectives, we went through four Design Cycles guided by the DSR process model proposed by Peffers et al. (2007) (see Figure 2). Each Design Cycle consists of three steps: design – build – evaluate. The evaluators for each cycle were academics or practitioners with cyber resilience expertise. For feedback gained from evaluators, we analysed them in the following design steps, then implemented feedback that improves the usability of the artefact.

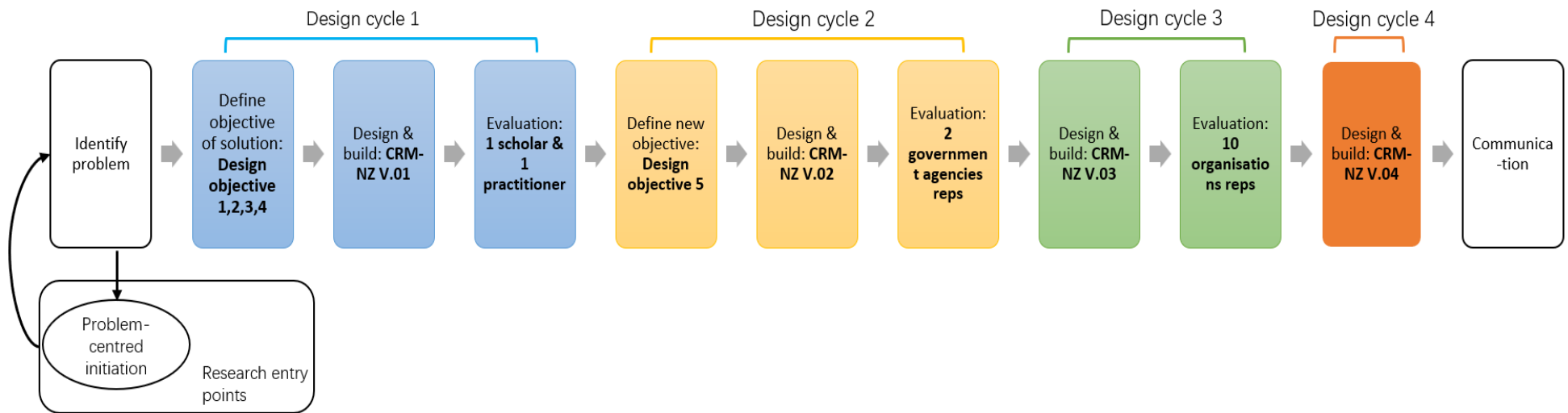


Figure 2: Design cycles of research (Adopted by Peffers et al., 2007).

5.1. Design Cycle of Iteration 1

5.1.1. Designing CRMAM V.01

Towards these objectives, we started the first Design Cycle. To have **a clear definition and comprehensive coverage of concepts** in cyber resilience (DO1), we decided to review the existing solutions provided in the knowledge base and identify the essential concepts in the cyber resilience area. Firstly, we created a weighting matrix to select suitable frameworks for review. The reason is that some well-designed frameworks are not broadly applicable to New Zealand organisations due to the unique characteristics of the New Zealand business environment.

For instance, the size of “small organisations” varies in New Zealand compared to some large countries. According to the NIST’s standard (Kissel, 2014), a small organisation is defined as a business “with up to 500 employees” (U. S. Small Business Administration, 2022, p.01). By contrast, organisations of the same size in New Zealand are grouped into “large organisations”. The “small organisations” in New Zealand, however, typically have 0 – 19 employees (King & Ockels, 2009). Meanwhile, although large organisations (100 or more employees) are growing clearly in recent years, 72% of organisations in New Zealand are one-men-band companies with no (paid) employees based on the statistics in 2022 (Statistics New Zealand, 2022).

In this case, the resources required to implement these professional and detailed frameworks remain beyond the reach of most organisations in New Zealand, even though some frameworks have modified versions available for “small organisations”. Therefore, we needed to filter the suitable frameworks for reviewing and capturing concepts. We proposed four selection criteria as outlined in Table 3.

Table 3: Selection criteria for framework review.

Criteria	Explanation
Dimension	<p>What approach does the framework use to make suggestions?</p> <ul style="list-style-type: none"> • Dimension 1: Cyber resilience lifecycle (predict, detect, withstand, recover, and evolve), e.g., Cyber resilience matrix. • Dimension 2: Areas that affect resilience, e.g., CRR. • Both: Both dimensions are considered, e.g., NIST CSF.
Target audience	<p>What is the target audience of the framework?</p> <ul style="list-style-type: none"> • Commercial: Target commercial companies. • Others: Such as government departments and the energy sector.
Implementation procedure	<p>Does the framework provide an implementation procedure?</p> <ul style="list-style-type: none"> • Provided • Non-provided
Focus	<p>Is the framework designed by focusing on cyber resilience or only covering parts of cyber resilience?</p> <ul style="list-style-type: none"> • Generic: Focus on all areas. • Non-generic: Focus on one or a few subsections.
Source type	<p>What is the source type of the framework?</p> <ul style="list-style-type: none"> • Standard: Frameworks are designed and used by the standard body. • Whitepaper: Frameworks are designed and utilised by government-funded research groups or government agencies. • Academic: Frameworks are designed and used by academics. • Commercial: Frameworks are designed and used by commercial businesses.

However, the current criteria were insufficient during the initial review. While they were able to highlight some characteristics of the reviewed frameworks, which facilitated our understanding of the entry point and designers' purpose, the criteria did not shape the differences in the utilisation of frameworks. Therefore, under the guidance of two experts in the field of cyber resilience, we added some new criteria and explained them in Table 4.

Table 4: New selection criteria for framework review.

Criteria	Explanation
Publish/update year	What is the public year of the framework? Has it been updated after publishing?
Issuing authority	What is the issuing authority of the framework? <ul style="list-style-type: none"> • Standard body: Issued by formal institutions. • Government: Issued by government agencies. • Academic: Issued by academics. • Commercial: Issued by commercial organisations.
Actively used	Has the framework been actively used by organisations? <ul style="list-style-type: none"> • Yes • No
Breadth of usage	What is the breadth of usage? Is it used in a particular area or widely across different sectors/industries? <ul style="list-style-type: none"> • Broad: The framework has been broadly used across organisations or industries. • Limited: The framework has only been used in specific organisations or industries.

After adding the new criteria, we combined all selection criteria together and additionally created the weighting matrix. For types in each criterion, we weighted them differently (see Table 5).

Table 5: The weighting matrix.

Weighting	1	2	3	4
Publish/update year	Before 2012	2012-2017	2018-2023	
Issuing authority	Commercial	Academic	Government	Standard Body
Actively used	No	Yes		
Breadth of usage	Limited	Broad		
Source type	Commercial	Academic	Whitepaper	Standard
Dimension	1 or 2	Both		
Target audience	Others	Commercial		
Implementation procedure	Non-provided	Provided		
Focus	Non-generic	Generic		

For the **year of publishing and updating**, capturing them provides a good indication of the relevance

of frameworks to the current situation. Some well-designed frameworks proposed long ago may not be a suitable solution to the problems encountered recently because the situation they addressed might have changed over time. We tend to allocate the highest weighting to frameworks published or updated within the last five years. For **issuing authority**, while reviewing the knowledge base, we found that besides the intense collaborations among academics, some governments also participate in cyber resilience framework design. Since the frameworks created by commercial companies are often revenue-oriented and likely describe events with a biased view. This category (commercial) has the lowest weighting. Conversely, standard bodies target entities all over the world. We considered them the most objective designers, therefore ranked them with the highest weighting.

For **actively used**, this criterion clearly distinguishes which frameworks are widely accepted by organisations and governments. Although some frameworks are proposed by authoritative bodies, they are abandoned by organisations for several reasons (e.g., hard to adapt, time-consuming and effort-consuming) (Kosutic & Pigni, 2022). So, the frameworks generally accepted and used by organisations have a higher weighting. For **breadth of usage**, some frameworks are only well-used in a particular area because the framework is designed specifically towards that area (Dupont, 2019; Ganin et al., 2020). Some frameworks are modified by government agencies with consideration heavily for their local environment (AEMO, 2021) and may not suit organisations in countries that do not share similar environmental characteristics, such as AESCSF (AEMO, 2021). We tend to allocate the frameworks designed for broad scope higher weighting.

For **source type**, we considered the frameworks proposed and used as the standard across the industries to have the highest weighting as their usefulness and acceptance have been proven in real-world environments. By contrast, the frameworks designed and used only by an individual or small group of researchers have lower relevance and therefore have a lower weighting as they may not be tested with enough practitioners. For the **target audience**, some frameworks only targeted specific industries when providing advice, such as government departments (Linkov et al., 2013) and commercial companies (Benz & Chatterjee, 2020). Because the target audience of our artefacts is general commercial organisations, frameworks designed for commercial organisations are appropriate to be considered as the basis for building our artefacts, thus having a higher weighting.

Suggestions of **implementation procedure** can effectively improve the accuracy of communication

and information transformation when multiple parties are involved in cyber resilience management. We gave frameworks that have such suggestions a higher weighting. For **focus**, some frameworks addressed specific areas of cyber resilience (e.g., risk assessment). Ideally, we think the frameworks with a generic focus should have higher weighting as they assist organisations in assessing their levels comprehensively. With these considerations in mind, we listed the categories and assigned a weighting value against each criterion as outlined in Table 5.

With this weighting matrix and the selection criteria considerations, we had a method whereby allowed us to determine which frameworks had the highest score to be the best candidates that we would work with moving forward. We selected five frameworks with the highest aggregate scores:

1. **Cyber Resilience Review:** It helps measure organisational resilience and provides suggestions for improvement by analysing the affected factors (CISA, 2020b).
2. **Cybersecurity Capability Maturity Model:** It helps users measure their capabilities and set goals and priorities for improvement (Muneer, 2022).
3. **NIST Cyber Security Framework:** It identifies 108 practices and provides detailed explanations by five phases associated with cyber security activities (NIST, 2018).
4. **CERT Resilience Management Model:** It helps "make operational resilience a repeatable, predictable, manageable and improvable process" (Caralli et al., 2016, p.1165) from 12 aspects.
5. **Australian Energy Sector Cyber Security Framework:** It aims to help Australian energy sector stakeholders use C2M2 to improve resiliency (AEMO, 2021).

To organise and compare the characteristics of these five frameworks clearly and concisely, we used the concept-centric matrix (named as "baby-step") to process the captured information of these five frameworks (as shown) in Table 6. A concept-centric matrix is a grid-based tool used in academic research to organise and categorise ideas and concepts by breaking down complex information into manageable pieces (Goldman & Schmalz, 2004; Morakanyane et al., 2017). The baby-step matrix only contains the attributes of reviewed frameworks corresponding to the criteria we discussed above. This provided us with a way to compare the features of frameworks and obtain a high-level understanding of them to prepare an in-depth review of the frameworks in the next step.

Table 6: Concept matrix for reviewed frameworks (baby-step).

Framework name	Cyber Resilience Review (CRR)	Cybersecurity Capability Maturity Model (V.2.1) (C2M2)	NIST Cyber Security Framework (NIST CSF)	CERT Resilience Management Model (V.1.2) (CERT-RMM)	Australian Energy Sector Cyber Security Framework (ADESCSF)
Publish year	2014	2014	2014	2010	2018
Update year	2020	2022	2018	2016	2022
Issuing authority	Government	Government	Government	Academic	Government
Actively used	Yes	Yes	Yes	Yes	Not Sure
Breadth of usage	Broad	Broad	Broad	Broad	Limited
Source type	Whitepaper	Whitepaper	Standard	Whitepaper	Whitepaper
Dimension	2	2	Both	2	2
Target audience	Companies	Companies	Critical infrastructures	Companies	Energy sector
Implementation procedure	Provided	Provided	Provided	Non-provided	Provided
Focus	Generic	Non-generic	Generic	Generic	Generic

After briefly reviewing these five frameworks, we found two with high similarities: C2M2 and ADESCSF. C2M2 is a model created in 2014 and updated in 2022 by American public- and private-sector organisations (Muneer, 2022) to assist users in measuring their capabilities and setting goals regarding cyber security (Muneer, 2022). Similarly, ADESCSF is a framework created in 2018 and updated in 2022 by Australian government and representatives from energy organisations. It covers the concepts recognised among many well-used frameworks and links to Australian-specific control references (AEMO, 2021). We noticed that ADESCSF was designed based on C2M2. The designers of ADESCSF made the specialist adaptation of C2M2 to allow the Australian energy sector businesses to use C2M2 and guide their practices. The concepts mentioned in these two frameworks overlap significantly. Therefore, we deducted ADESCSF from our reviewed framework scope.

To compare the rest of the frameworks, we extended the concept matrix from baby-step to adult-step. We used it to help categorise related concepts and identify their connections. This concept matrix contains two parts: concepts mentioned by these frameworks and markers representing the similarities and differences of concepts.

Firstly, we used CRR as a standard to capture the related concepts and compare them with other frameworks that have been reviewed. We chose CRR as the standard because CRR is not only a well-used framework and has proven its applicability across industries and countries, but also a lightweight assessment method that covers only the most fundamental domains of cyber resilience (CISA, 2016b, 2020b).

Secondly, three types of markers are used in this matrix (Table 7). Using distinguishable markers is because many frameworks discuss different scopes of concepts despite the same nomenclature being used. A specialist distinction has been made to each domain within each framework to describe the concepts accurately.

Table 7: Markers and meanings for framework reviewing.

Markers	Meanings
X	This domain has the same name and concept as the CRR domain.
!	This domain has the same concept as the domain in CRR but is named differently.
#	This domain discusses the same content as the domain in CRR but is grouped as a sub-domain in another domain.

We gathered the concepts proposed in CRR as the foundation of the concept matrix (adult-step) and then compared the concepts mentioned in the other three frameworks (see more framework comparison details at <https://osf.io/q7gpx/files/osfstorage/649bd397a2a2f40d3a4366e6>). If a concept is mentioned in both frameworks, we mark them with three markers in the concept matrix according to concept details. For any new concepts outside the coverage of CRR are proposed, we analysed and added them as a new item to the concept matrix. We compared the frequency and scope of each concept mentioned in the reviewed frameworks and developed the concept matrix from baby-step to adult-step (Table 8).

Table 8: Concept matrix for reviewed frameworks (adult-step).

Framework name	Cyber Resilience Review (CRR)	Cybersecurity Capability Maturity Model (V.2.1) (C2M2)	NIST Cyber Security Framework (NIST CSF)	CERT Resilience Management Model (V.1.2) (CERT-RMM)
Concept 1	Asset Management	#	X	X
Concept 2	Controls Management	!	!	X
Concept 3	Configuration and Change Management	#	!	
Concept 4	Vulnerability Management	X	#	X
Concept 5	Incident Management	#	!	X
Concept 6	Service Continuity Management	#		X
Concept 7	Risk Management	X	!	X
Concept 8	External Dependencies Management	X	!	X
Concept 9	Training and Awareness		X	X
Concept 10	Situational Awareness	X		
New concept1		Workforce Management		!
New concept2		Information Sharing and Communication	X	X
New concept3		Cyber Security Program Management		
New concept4			Governance	X

Note:

- X: This domain has the same name and concept as the CRR domain.
- !: This domain has the same concept as the domain in CRR but is named differently.
- #: This domain discusses the same content as the domain in CRR but is grouped as a sub-domain in another domain.

Ten concepts were mentioned in more than half of the reviewed frameworks: asset management, controls management, configuration and change management, vulnerability management, incident management, service continuity management, risk management, external dependencies management, training and awareness, and information sharing and communication. We did an in-depth analysis of all concepts identified in the concept matrix and decided on the domains that should be included in our methodology in the building phase.

5.1.2. Building CRMAM V.01

We analysed the concepts identified in the previous phase and their coverage and started building our solution: Cyber Resilience Maturity Assessment Methodology (CRMAM). The first finding we obtained is that the grouping of domains varies significantly. Unlike some popular concepts (e.g., asset management) are suggested by all frameworks as separate domains, some important concepts (e.g., information sharing and communication) are scattered across several domains as sub-domains, which may lead organisations to underestimate the importance of these concepts. In addition, as mentioned earlier, inconsistent naming nomenclature is also a significant problem. These inconsistencies add barriers to understanding and using frameworks by organisations, making it difficult for them to determine whether they understand the concept correctly.

To solve these problems, we consolidated all concepts into the resulting ten concepts described below. We use “domain” to refer to these concepts, as this term is well-used across the reviewed frameworks. It means “a logical grouping of cybersecurity practices that contribute to the cyber resilience of an organisation” (CISA, 2020, p.47).

1. Asset management

Asset management refers to organisations’ actions to identify, record, and manage critical assets. The assets are mainly classified into four categories: people, information, technology, and facilities (CISA, 2016a, 2020b). In asset management, organisations need to identify precisely what assets are required and reasonably plan them to improve the resilience of critical services, which can be seen as the foundation for building cyber resilience. Most frameworks suggest that organisations put extra protection around assets related to critical services and maintain inventories periodically (CISA,

2020a; Fielder et al., 2016; NIST, 2018). It is worth noting that information assets are one important aspect to focus on. Managing an organisation's information assets revolves around confidentiality, integrity and availability (CIA triad) (Carías, Borges, et al., 2020). Information protection should be prioritised according to the attributes of the information asset (Caralli et al., 2016).

2. Controls management

Controls management aims to secure critical services by identifying, analysing, and managing operational environments that can affect them, such as personnel access to data, physical monitoring of critical equipment, and audit of internal asset usage. Many frameworks emphasise the importance of access controls in this area. In C2M2 v.2.1, for example, the designers emphasised that access requirements should be associated with assets and that organisations should regularly review access requirements to determine the validity of access rights (Curtis et al., 2015). In addition, frameworks also point to the need to use diverse methods. CRR suggested using CCTV for physical monitoring (CISA, 2020a). CR-SAT (Carías et al., 2021) and CRPM (Carías, Arrizabalaga, et al., 2020) suggested creating integrity-checking mechanisms for identity management in the latest versions.

3. Configuration and change management.

Configuration and change management is essential in securing cyber resilience in most reviewed frameworks. The study refines it as an organisation's actions to respond to changes and reallocate resources. Frameworks generally agree on the need for ongoing management and maintenance of assets, risks, and other relevant factors in this domain (Caralli et al., 2016; CISA, 2020b). Organisations should monitor assets and make proper adjustments to cope with new changes in operational environments. Some frameworks emphasised the need to continuously audit changes in all domains of cyber resilience (Curtis et al., 2015; Muneer, 2022). Meanwhile, some frameworks, such as CERT-RMM, and NIST CSF, arguably included it in asset management and controls management (Caralli et al., 2016; NIST, 2018) as they mainly focus on managing changes in assets, from storage status (e.g., paper-based to electronic-based) to their relationships (e.g., ownership, custodianship) (Caralli et al., 2016).

4. Governance

Suggestions in whitepapers about “governance” are scattered and discussed in different areas. They include three areas: 1) Create and implement relevant policies and guidance (e.g., CR-SAT, CRPM,

NIST CSF, Cyber Resilience Matrix). Although the frequency of references varies, most suggest organisations create policies for guiding practices, which is also agreed upon in academic articles (Carias et al., 2021). 2) Apply continuous improvements from lessons learned (e.g., CRPM, ISFAM). Some frameworks see the need for periodic reviewing of related practices to apply lessons learned previously to new practices. 3) Flexibly adapt and reallocate resources (e.g., CRPM, CR-SAT, CMAF). Some frameworks also grouped resource reallocating and realigning into the “governance” domain. Combining these three areas, this study argues that governance refers to the actions of an organisation to guide cyber resilience practices and respond to change. It reflects the level of organisational engagement in cyber resilience and the corresponding management behaviours (Carías, Arrizabalaga, et al., 2020; Carías, Borges, et al., 2020).

5. Vulnerability management

Vulnerability management focuses on organisations’ actions to identify, analyse, manage, and respond to threats and vulnerabilities in their operational environments. Vulnerabilities inevitably arise when exchanging and using organisations’ business data and personal information. The root causes of these vulnerabilities are various, ranging from those caused by outdated technology to human mistakes (Williams & Manheke, 2010). Most of the reviewed frameworks agreed with running vulnerability checking and management. Some academics argued that lowering the vulnerability level is vital to improving cyber security, but it does not mean all vulnerabilities must be treated equally (Galinec & Steingartner, 2018). Organisations should pay more attention to vulnerabilities in critical components related to key services while policing vulnerabilities in other endpoints.

6. Incident management

Incident management is mentioned in all reviewed frameworks, which illustrates the importance of this aspect. Incident management refers to an organisation’s preparedness to face possible incidents and to detect, respond and recover from them when they occur. Some frameworks also emphasised the need for evaluation and lessons learned after an incident, such as the cyber resilience matrix, CRPM, and CR-SAT. Most of these frameworks divided incident management into five steps according to the incident lifecycle: 1). *Prepare*: anticipating possible risks, vulnerabilities and attacks before incidents and designing response plans (Annarelli & Palombi, 2021); 2). *Detect*: investigating incidents and determining whether they relate to other events (Benz & Chatterjee, 2020); 3).

Response: maintaining operational needs and withstanding attacks during events (Alexander Kott & Linkov, 2019); 4). *Recover*: restoring damaged services and functions after events (Onwubiko, 2020b); 5). *Absorb*: learning lessons from cyber incidents and improving existing technologies (Carías et al., 2018).

7. Service continuity management

Service continuity management refers to organisations' actions to keep providing service during and after an incident. It focuses on the detection, response, and recovery phases (CISA, 2020a; Onwubiko, 2020b). Due to capability limitations, some SMEs must stop service to focus on mitigation when incidents occur. This forces them to suffer the pain of financial losses and trust crisis from customers, which can be as damaging as the "aftershocks" of the earthquake. Therefore, these types of SMEs must have a business continuity plan in place. While continuity management and incident management both revolve around the occurrence of and response to cyber incidents, service continuity management focuses on defining and implementing plans to make critical services as unlikely as possible to be affected and to maintain functionalities continuously (Onwubiko, 2020b) rather than analysing incident to create proper remediation plans.

8. Risk management

Risk management is about the actions that organisations take to improve their ability to identify risks and reduce stress in the face of cyber incidents. The importance of risk management is reflected in most academic studies. The measurements of cyber risk used in these studies are based on the probability of an incident occurring and the impact of the incident (Linkov & Kott, 2018). Since risks are unavoidable, even if individual risks can be remediated through measures, the information exchange in an organisation's business activities can still pose potential risks (Linkov & Kott, 2018). Therefore, the main objective of risk management should be to improve the ability to identify risks in advance and take measures to reduce the pressure and control identified risks.

9. External dependencies management

External dependencies management refers to the actions that organisations take to establish good cooperation with external stakeholders and manage risks. Although most frameworks mentioned this, they did not discuss it as a separate domain. CR-SAT and CRPM described identifying internal and external dependencies of organisational assets in "Asset Management" (Carías et al., 2021;

Carías, Arrizabalaga, et al., 2020). This study argues that external dependency management should be as important as other areas, as organisations need to monitor the external environment and collaborate with all relevant stakeholders to ensure resilience (Caralli et al., 2016). Communication is also an essential section within this domain. Organisations need to build cooperative relationships with other related parties. As computer systems are often interdependent (Ganin et al., 2020), it is difficult to disconnect and avoid affecting other systems promptly when an incident occurs (Dupont, 2019; Linkov & Kott, 2018; Zemba et al., 2019). Effective and timely communication is one of the key elements to support organisations in determining the status of an incident.

10. Training and awareness

Training and awareness refer to the actions that organisations take to develop cyber security awareness of human aspects to support critical service. Many academics emphasised that human-caused failures remain one of the leading causes of cyber incidents in their studies (Andronache, 2021). Linkov et al. (2013) argued that organisations should shift cognitive biases and establish a cyber-aware culture, and staff's readiness to respond to incidents needs to be regularly assessed. It is worth noting that although "workforce management" – tracking and managing employees' lifecycle for specialist training – is only mentioned in two of the reviewed frameworks (C2M2, CERT-RMM), this concept is advocated as a novel way to increase their cyber resilience awareness for employees at different stages of roles.

In contrast to the ten domains identified in the previous phase, our methodology does not include "information sharing and communication" as a separate domain. We argue that information sharing should be considered on a broad level. For example, in the area of incident management, where organisations should respond to cyber incidents and share information with potentially affected parties on time. Similarly, in external dependencies management, organisations should establish efficient information sharing and cooperation with external dependencies to obtain timely intelligence.

Meanwhile, we noted that governance is discussed as a sub-area in many frameworks, underestimating the importance of governance in cyber resilience management. At a macro level, organisations need guidance from top management to identify key resource areas and assets that need to be prioritised for protection. At a micro level, every control implemented by organisations

needs to be reviewed regularly to achieve compliance and meet control objectives. Governance, therefore, plays a leading and guiding role in organisations to improve their cyber resilience. During the course of this study, we noted that the new version of NIST CSF in draft and review also indicated that “Governance” needs to be pulled out as a domain in its own right. To respond to this, we added “governance” as a separate domain in the methodology.

After building the domains, to achieve the needs of having **essential cyber resilience practices and detailed descriptions** (DO2), we carried out another round of analysis around the practices suggested in the reviewed frameworks. Firstly, we extracted all practices related to the ten domains identified from all reviewed frameworks and got 896 practices. Duplicate practices were eliminated through detailed reading. After analysing the remaining practices, we extracted the core elements organisations had to consider in each domain and framed them in a mind map (see Figure 3). After twice checking and evaluating iterations of the mind map, we developed practices for each domain, a total of 52 practices. It is worth noting that during our analysis of each practice, the crosswalk table (Homeland Security, 2014) provided by CRR on how practices linked with NIST, CERT-RMM and other relevant references played a clear role in helping us to determine how the practices were linked across frameworks more accurately. This experience also reinforced our design objective of **adding corresponding references** (DO3) to the CRMAM.

After identifying the practices included in the CRMAM, we added **a corresponding reference for each practice** (DO3) that echoed the practices in the reviewed frameworks. The goal is to assist organisations in understanding how each practice maps across these frameworks. Moreover, if organisations’ existing practices are created based on one or multiple reviewed frameworks, these links can also assist them in accurately understanding and efficiently evaluating the corresponding practices in CRMAM. In the process of adding references, we did a second comparison and analysis of all the practices, and 8 of them were removed because the four frameworks did not widely propose them, we did not consider them to be generic. The CRMAM V.01 is shown in Figure 4 (you can find the full version here <https://osf.io/q7gpx/files/osfstorage/649bd88a6513ba0c4b3a3be4>).

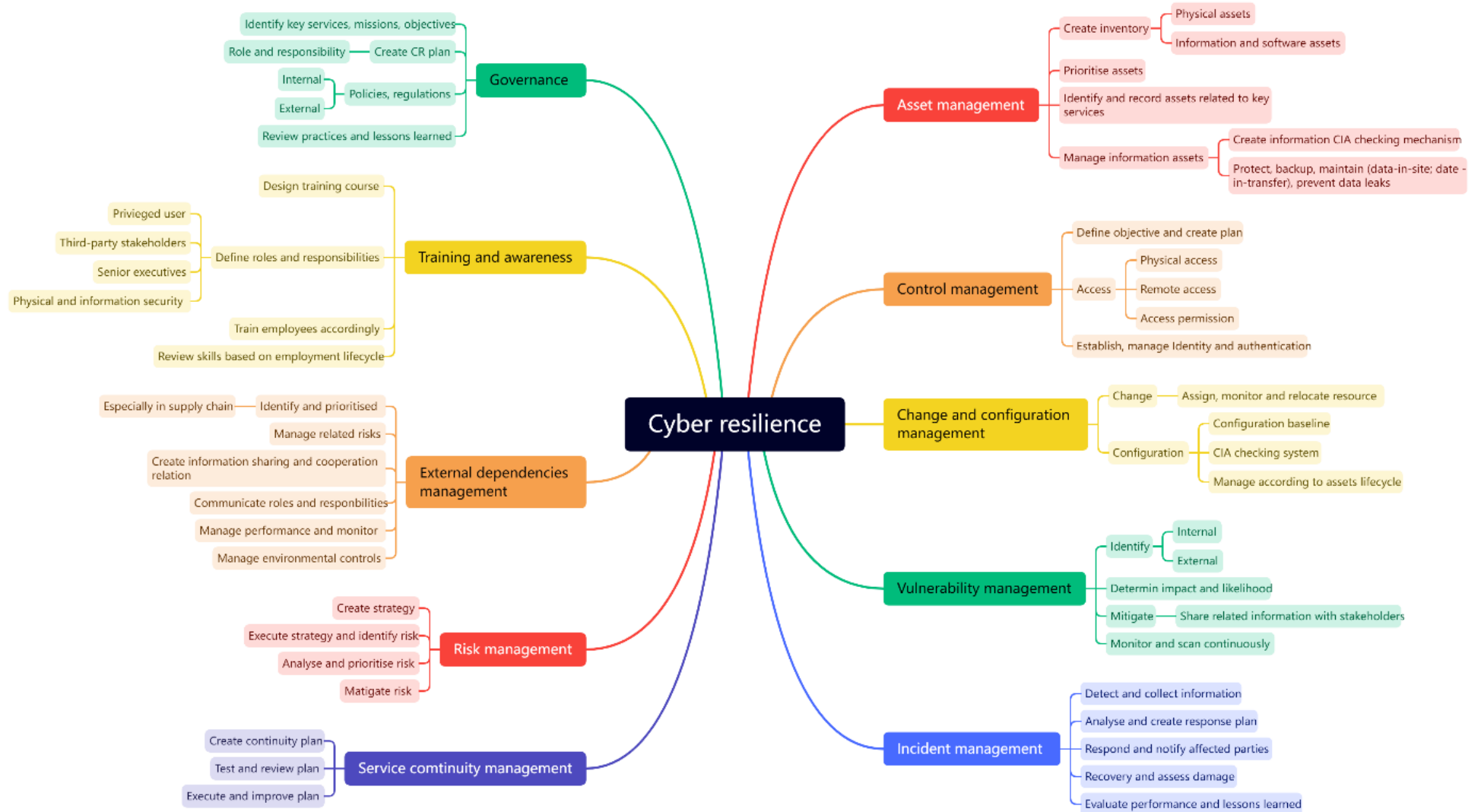


Figure 3: Mind map for concepts and their core elements.

Domain	Definition	Practices	CRR	C2M2	NIST	CERT
Asset management	It refers to the actions the organisation takes to identify, record and manage the organisation's critical assets.	Identify and record key critical services (mission, objectives, and activities) and related assets.	AM.G1	ASSET.OB1a,e	ID.AM6	ADM.SG2.SP1
			AM.G2			ADM.SG2.SP2
			AM.G2			
		Identify and establish physical asset inventory with specific details.	AM.G3	ASSET.OB1f,g,h	ID.AM1	ADM.SG1.SP1
			AM.G4			
			AM.G7			
		Identify and establish software and information asset inventory with specific details.	AM.G2	ASSET.OB2f,g,h	ID.AM2	ADM.SG1.SP1
			AM.G3			TM.SG1.SP1
			AM.G4		ID.AM4	KIM.SG4.SP3
			AM.G6		PR.DS3	KIM.SG1.SP1
		Prioritise assets based on their business value, classification, and criticality.	AM.G1	ASSET.OB1c ASSET.OB2c	ID.AM5	SC.SG2.SP1
			AM.G7			KIM.SG1.SP1
		Create information integrity checking mechanisms.	CCM.G2	ARCHITECTURE.OB2	PR.DS7	TM.SG4.SP3
			CM.G2		PR.AC5	KIM.SG5.SP3
						KIM.SG5.SP1
						KIM.SG5.SP2
				CTRL.SG2.SP1		
Implement measures to protect, back up, and maintain information assets and related activities.	AM.G6	ARCHITECTURE.OB2c,e,f	PR.DS1	CTRL.SG2.SP1		
	CM.G2		PR.DS2	KIM.SG4.SP1		
			PR.DS4	KIM.SG4.SP2		
			PR.DS5	KIM.SG4.SP3		
	CCM.G1		PR.IP4	TM.SG5.SP3		
				KIM.SG6.SP1		
				KIM.SG2.SP1		
Controls management	It aims to improve the security of critical services by identifying, analysing and managing the operational environment. Controls management focuses on the control of any factors that may affect the operational environment.	Define control objectives and design a control plan.	CM.G1	/	/	/
			CM.G3			
		Manage physical access to critical assets/services.	AM.G5	ARCHITECTURE.OB3a	PR.AC2	HRM.SG4.SP1
			CM.G2			AM.SG1.SP1
			CCM.G1	ACCESS.OB3	PR.MA1	ADM.SG3.SP2
		Manage remote access to critical assets/services.	AM.G5	ARCHITECTURE.OB3b	PR.AC3	HRM.SG4.SP1
			CM.G2			AM.SG1.SP1
			CCM.G1	ACCESS.OB2c	PR.MA2	ADM.SG3.SP2
			AM.G5	ARCHITECTURE.OB3a	PR.AC4	HRM.SG4.SP1
		Manage access permission and review periodically.	CM.G4			PR.PT3

< >

Concepts with practices

Sheet1

CRR

C2M2

NIST

CERT

+

Figure 4: Screenshot of CRMAM V.01 (partially).

5.1.3. Evaluating CRMAM V.01

As steps suggested by the DSRM process model (Peppers et al., 2007), the designed artefact must be evaluated by “well-executed evaluation methods” (Hevner & Chatterjee, 2010, p.83) to determine its “utility, quality, and efficacy” (Hevner & Chatterjee, 2010, p.83). After designing and building CRMAM V.01, we invited two experts in the cyber resilience area for evaluation. The evaluators consisted of an academic from computer science and a practitioner from the cyber resilience area. Both experts have commercial and IT experience across the government, public sector, and businesses in New Zealand. We believe that their academic and practitioner experience brings multiple angles to evaluation. These two experts’ expertise enables us to obtain a professional assessment of the CRMAM’s terminology and structure from an academic’s perspective, and a proper assessment of entry barriers and learning costs from a practitioner’s perspective. We also invited an academic from the information systems field who is familiar with the DSR approach to oversee the evaluation process to ensure the transparency and integrity of the interaction.

We demonstrated CRMAM V.01 to them and explained how we used the weighting matrix to filter the frameworks found from the knowledge base and designed CRMAM. After that, we held a focus group discussion. The group discussion was about 1.5 hours. The discussion contents were around four areas: 1) Whether the criteria and weighting of the weighting matrix are reasonable, 2) Whether the current CRMAM have reasonable coverage and a clear definition of the domains and practices, 3) Whether the descriptions and domain-centred groupings are reasonable, and 4) Whether any frameworks needed to be added to the scope of framework reviewing. Each practice was coded to be convenient for the experts’ assessment (see Figure 5). After group discussion, we obtained two notable findings in the assessment process.

Domain	Definition	Code	Practices
Asset management (AM)	It refers to the actions the organisation takes to identify, record and manage the organisation's critical assets.	AM1	Identify and record key critical services (mission, objectives, and activities) and related assets.
		AM2	Identify and establish physical asset inventory with specific details.
		AM3	Identify and establish software and information asset inventory with specific details.
		AM4	Prioritise assets based on their business value, classification, and criticality.
		AM5	Create information integrity checking mechanisms.
		AM6	Implement measures to protect, back up, and maintain information assets and related activities.

Figure 5: Code example of each practice.

Feedback 1. Categorising practices.

Improving cyber resilience is often not easily achieved by simply presenting the domains and practices for the target users. In most cases, organisations already have a basic understanding and use of frameworks around cyber resilience. However, as each framework has a different focus, organisations that have only adopted a single framework will not necessarily achieve the goal of improving cyber resilience comprehensively. For instance, Some frameworks (e.g., Cyber Resiliency Engineering Framework) provided many suggestions regarding specific controls (Bodeau et al., 2012). This may lead organisations that only use this framework as a guideline to neglect other aspects of cyber resilience management. To address this problem, we added an additional design objective – It should **categorise practices to assist organisations in understanding their strengths and weaknesses from high-level (DO5)**. The experts recommended categorising each practice. They summarised three areas that influence organisations’ operational behaviour: governance, operations, and controls as categorisations.

Feedback 2. Adding ISO27001

One of the experts in the evaluation suggested that ISO27001, as a global standard, is widely used and has proven its effectiveness. This international standard would not only add conviction to the existing designed methodology. It would also allow potential target users to compare their practices with those already in place and obtain more external references. As they suggested, we added ISO27001 to the framework reviewing scope.

5.2. Design Cycle of Iteration 2

5.2.1. Designing CRMAM V.02

Based on the feedback, we decided to redesign CRMAM V.01. In this iteration, we added one new feature to CRMAM to reflect the additional design objective and demonstrated CRMAM V.02 to government agency representatives for reasonableness evaluation.

To **categorise practices (DO5)**, we need to add categorisations for each practice. Initially, we tried categorising practices according to the definitions provided in the reviewed frameworks. However, their definitions are slightly different. The blurry among these definitions created obstacles to practice categorising. We agreed with the experts that having clear definitions and being aware of how they impact internally are constraints for correct categorisation. To meet these constraints and group the practices accurately, we conducted another literature review and then grouped the practices accordingly.

In most whitepapers and studies, designers provided suggestions for organisations around “governance”, “operations”, and “controls”. These definitions and interpretations with slight differences can often confuse users (von Solms & von Solms, 2018). Especially for top management in organisations that do not have a deep level of expertise, the convoluted explanations do not deliver to them the importance of three categorisations and how they can be used to address the challenges in cyber resilience. To ensure the rigour of categorisations’ definition, we first captured the descriptions provided in the literature via table to compare the differences. Some keywords were frequently mentioned in these descriptions. We then generated definitions based on these keywords in the organisational environment. A detailed explanation of each definition is discussed below.

5.2.1.1. Defining Governance

Both reviewed whitepapers and academic articles emphasised the importance and leadership of governance in organisations. We explained the impact of governance on organisational development and then discussed them in cyber resilience.

“Governance” is often discussed as being led by top management. In the business environment, governance usually refers to the set of initiatives exercised by the organisation’s Board (Bodeau et al., 2010). Most academics mentioned the importance of top management within organisations in making decisions, guiding direction, and providing oversight (Harris & Martin, 2021; Low, 2006). They argued that failures in governance are one of the root causes of significantly failed business activities. Therefore, this study defines “Governance” as follows:

“The processes that identify the key business services and business activities to evaluate risk and maturity and allocate priority for guiding operations about the focus areas.”

“Cyber security governance” is seen by academics and practitioners as an aspect of internet governance (Mueller, 2017). Some frameworks, such as CERT-RMM and NIST CSF, emphasise the importance of keeping organisations direction consistent with policies, regulations, and laws in their definitions. The academics generally emphasised the key role of top management in “cyber security governance” in their studies. Governance requires the involvement of top management in organisations (De Bruin & Von Solms, 2016). They need to become more aware of cyber resilience and remain sensitive to cyber-related information to support operations in line with relevant policies and changes in operating environments (Yusif & Hafeez-Baig, 2021).

The Board and top management are the main actors in implementing “governance”. Their decisions influence the allocation of resources and the focus on protection in organisations regarding cyber resilience management (Yusif & Hafeez-Baig, 2021). However, some academics pointed out in studies that organisations, especially SMEs, lack an understanding of cyber security at the Board and senior management (Musa, 2018), which often leads to a lack of involvement in cyber resilience governance. An EY survey of 2020 showed that only 42% of managers claim their Boards are fully involved in developing security strategies (Ernst & Young, 2020). This also leads to organisations being unable to allocate resources and hedge risks effectively. Therefore, some academics stated that “cybersecurity and resilience are all about governance” (North & Pascoe, 2016. p.146).

5.2.1.2. Defining Operations

Similarly, definitions of “Operations” were captured from whitepapers and studies. We found it hard to find the specific definition of “operations” in related materials, it is mainly referred to in the

context of “operational resilience”, but despite this, we could discern the primary function of operations for allocating resources in mitigating risk and maintaining business activity from the descriptions collected.

Operations refer to organisations adopting strategies in business activities to analyse market and customer needs and develop products to increase sales. This range of business activities can all be considered part of operations. This study defines “Operations” to be:

“The combination of people, processes, and controls to manage and mitigate the risk of business services and maintain business activities.”

Organisations optimise processes to utilise information and assets and transform them into products and services with the help of technology in operational activities. Operations thus express the coordinated cooperation of processes, people, resources and organisational management (Ruffini et al., 2000). In contrast, cyber security operations are not clearly defined in many studies and whitepapers. It is often understood as part of the daily business operations of organisations. Onwubiko (2020a) considered cyber security operations to be “broad and diverse” (p.86). It comprises four key responsibilities: administration, execution, monitoring and support (Onwubiko, 2020a). These tasks can be undertaken by individuals within organisations by teams or even outsourced to specialist providers.

Cyber security operations are at the core of an organisation’s security activities (Cogburn, 2022). Organisations use assets to sustain their business operations; assessing these assets and mitigating vulnerabilities is key to optimising the efficiency of organisations’ business activities. In response, some academics suggest establishing operational security programmes to monitor, prevent, and detect cyber threats all day (Onwubiko, 2015). However, the lack of suitable solutions means needing to experiment and adjust constantly according to their needs, resulting in additional investment costs and ongoing maintenance expenditures. Therefore, some organisations may consider themselves the lucky outlier that are unsusceptible to cyberattacks, and neglect to pay attention to operational security.

5.2.1.3. Defining Controls

Controls as a popular area are discussed in most studies and whitepapers. Many cyber security frameworks make extensive recommendations for controls. Commercial organisations in the marketplace are also developing improvements around various control techniques. Based on the collected descriptions of controls, it appears that the manifestations of controls are varied, including tools, methods, procedures, actions, and other physical means.

Most studies described “controls” as “safeguards or countermeasures” based on equipment, technology, and management tools (ISACA, 2018; Krumay et al., 2018). Borky & Bradley (2019) specified “controls” further as “measures that mitigate a vulnerability to reduce risk” (p.349). This study defines “Controls” as:

“A set of tools, methods, procedures, and actions that should be taken by organisations to protect business services and business activities.”

This toolset can be administrative, technical, managerial or legal (ISACA, 2018). In cyber resilience, controls aim to avoid cyberattacks using risk management tools (Krumay et al., 2018). Some organisations improve information confidentiality by using physical methods such as biometric access control systems, while others improve security by administrative means such as establishing policies. To some extent, the actor of controls is not limited to the management level, employees can also use equipment and technology to achieve controls goals (Pawar & Palivela, 2022).

Given the rapid increase in cyberattacks, organisations continuously invest in control technologies. However, due to the complexity and rapid evolution of new technologies, it is not unusual for organisations to fail to keep up with innovations and take full advantage of the technology’s capabilities (Eaton et al., 2019). Eaton et al. (2019) highlighted the need to design effective controls for organisations rather than just trying to catch up with “new” technologies thoughtlessly. Furthermore, organisations must also review implemented controls periodically, so cyber exercises have been recommended by many academics recently (Gafic et al., 2022, 2021). Organisations test the maturity and reliability of response plans by simulating possible events or even hiring external ethical hackers to attack organisations.

5.2.1.4. Defining Relationships of Categorisations

While capturing and analysing the definitions of the three categories, we also paid attention to their relationships. We created a relationship map (see Figure 6) to illustrate their relevance and connections to each other and to visualise how the three categories inform and interact.

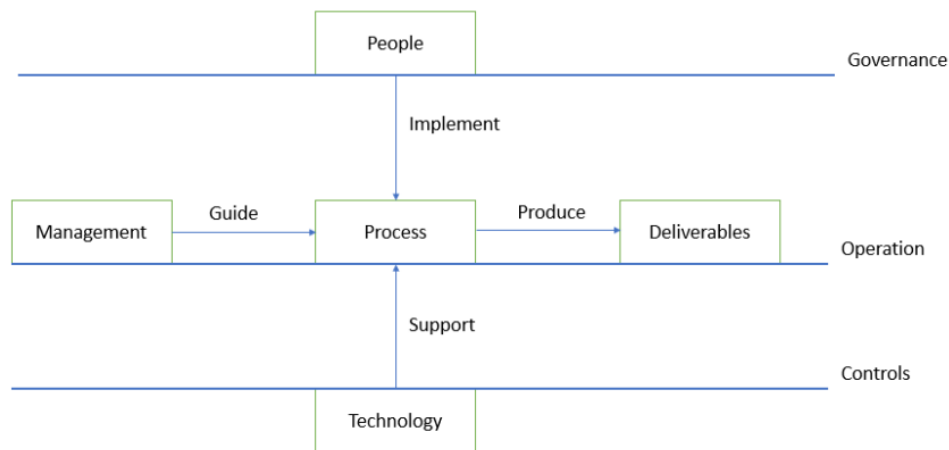


Figure 6: The relation maps for categorisation.

We considered this map the environment and relationships of organisations. It contains three categorisations: governance, operations, and controls. Each category contains single or multiple components associated with organisations and affected interactively. Governance is often the top management or the Board, defining purpose, providing direction, identifying priorities, and clarifying the organisation’s mission (Musa, 2018; von Solms & von Solms, 2018). Operations perform an integral part of managing and executing the organisation’s day-to-day business activities in response to the direction set by the Board. Managers set specific management strategies based on the direction provided by the Board and apply them in operations to guide processes (Musa, 2018). Controls provide technical support, employees can produce the product through the process (Chandra & Kumar, 2018). These three categorisations also play important roles in organisations’ cyber resilience management. Organisations use infrastructure and assets to secure their cyber operations, while top management monitors and adjusts based on new operations changes. Mindlessly strengthening single security control does not lead to efficient cyber resilience performance, so academics emphasised that “spending alone is not the solution to cyber security” (Arora et al., 2004; Fielder et al., 2016).

We also have an interesting metaphor to describe their relationship. If we think of an organisation as a vehicle, “governance” is the “driver” of this vehicle; it guides the vehicle and makes decisions at the critical point and is responsible for monitoring all aspects of the vehicle’s status from a high level to ensure it remains safe. “Operations” provide the “energy” for the vehicle. By using the infrastructures provided by “Controls” (e.g., technology, equipment), organisations carry out practices related to cyber resilience under the guidance of “drivers” and uses the feedback from these practices to improve “Governance”. “Controls” are the vehicle’s “wheels”. Organisations improve vehicle safety by improving their technology and management resources through physical and administrative means (such as adding access control and making policies).

5.2.2. Building CRMAM V.02

Based on the definitions mentioned above, we refined the CRMAM V.01 with the further assistance of the two experts we mentioned in the first evaluation phase.

Improvement 1. Add categorisation for practices.

To categorise practices, firstly, we added a column to CRMAM V.01 and set up a drop-down list for each cell, which had only four values to choose from: “governance”, “operations”, “controls”, and “N/A”. We added a few more columns to it, where evaluators could add comments, and asked the experts to evaluate each practice according to their view of where it should fit. To guarantee the objectivity of the results, the experts were not allowed to see each other’s answers during self-evaluation. Secondly, we explained to the experts how to use new columns and the expected results. Finally, we collected feedback from all experts and summarised it in a table. Interestingly, in the first aggregation, we found that all experts held only 16/44 categorisations in unison. A focus group discussion was then held to address the differences in the categorisation results. With the definitions of the three categories once again highlighted, 26 classifications were harmonised. A second focus group discussion was held to address and harmonise the remaining practices.

We conducted one-to-one interviews for the second group discussion with the same practitioner and academic whom we invited for the first evaluation. Before the interviews, we provided the experts with worksheets containing each other’s perspectives. The reason for doing this was to allow them to gain insights into each other’s different views and to provide them with the space to think

independently and thoughtfully before the interview. As the practitioner's daily work is closely related to the cyber resilience domain and similar products and frameworks, we interviewed the practitioner primarily and allowed the academic to confirm the categorisation results. In discussion with the practitioner, we revisited the categories for each practice and generated the results. The categorisations of 18 practices were then redefined during the interviews. Meanwhile, with the practitioner's assistance, we amended the descriptions of some of the practices to make them more accurate and to distinguish the categories clearly.

Improvement 2. Add ISO 27001 as the reviewed framework.

To include ISO 27001 in the methodology, we tried to find the content of ISO 27001. Unfortunately, the official content can only be obtained with adequate financial support. Other available materials are secondary interpretations of ISO 27001; their accuracy is not guaranteed. We therefore chose to use the crosswalk provided by CRR as the basis for our review because the artefacts provided by CRR are accurate and trustworthy as a standard used worldwide. This crosswalk compared suggestions of CRR and NIST CSF to ISO/IEC 27001:2013 and listed each corresponding suggestion in ISO/IEC 27001:2013 as one of the informative references (Homeland Security, 2014). We compared the practices in CRMAM with the practices and references in the crosswalk, then added a column of the corresponding references on ISO 27001 in CRMAM V.02. The CRAMA V.02 is shown in Figure 7 (you can find the full version here <https://osf.io/q7gpx/files/osfstorage/649bd3b56513ba0c543a32e4>).

Domain	Definition	Code	Categories	Practices	References		
					CRR	C2M2	NIST
Asset management (AM)	It refers to the actions the organisation takes to identify, record and manage the organisation's critical assets.	AM1	Operation	Identify and record the assets related to key critical services.	AM.G1	ASSET.OB1a,e	ID.AM6
					AM.G2		
		AM2	Operation	Identify and maintain physical asset inventory with specific details.	AM.G2	ASSET.OB1f,g,h	ID.AM1
					AM.G3		
					AM.G4		
					AM.G7		
		AM3	Operation	Identify and maintain software and information asset inventory with specific details.	AM.G2	ASSET.OB2f,g,h	ID.AM2
					AM.G3		
					AM.G4		ID.AM4
					AM.G6		PR.DS3
		AM4	Operation	Prioritise assets based on their business value, classification, and criticality.	AM.G1	ASSET.OB1c	ID.AM5
					AM.G7	ASSET.OB2c	
Controls management (CM)	Control management aims to improve the security of critical services by identifying, analysing, and managing the operational	AM5	Control	Create information confidentiality, integrity, and availability (CIA) checking mechanism.	CCM.G2	ARCHITECTURE.OB2	PR.DS7
					CM.G2		PR.AC5
		AM6	Control	Implement measures to protect, back up, and maintain information assets and related activities.	AM.G6	ARCHITECTURE.OB2c,e,f	PR.DS1
							PR.DS2
							PR.DS4
					CM.G2		PR.DS5
					CCM.G1		PR.IP4
		CM1	Operation	Define control objectives and design control plans.	CM.G1	/	/
					CM.G3		
		CM2	Operation	Manage physical access to critical assets/services.	AM.G5	ARCHITECTURE.OB3a	PR.AC2
					CM.G2	ACCESS.OB3	PR.MA1
		CM3	Operation	Manage remote access to critical assets/services.	AM.G5	ARCHITECTURE.OB3b	PR.AC3
					CM.G2		

Figure 7: Screenshot of CRMAM V.02 (partially).

5.2.3. Evaluating CRMAM V.02

As in Design Cycle 1, following the step mentioned in the DSRM process model (Peppers et al., 2007), we needed to demonstrate and evaluate artefacts again. For this round of evaluation, we decided to approach government agency representatives to evaluate the validity of the artefacts for a “reasonableness” test to determine whether our methodology makes sense to them. The reasons for contacting government agencies were twofold: firstly, because of the specific focus of their work and experience of working with other organisations, they have access to a broader range of data about organisations’ response methods and cyber incidents nationwide. Secondly, representatives from government departments are concerned with cyber resilience. They are familiar with government regulations of cyber resilience, which can provide an assessment regarding whether the methodology has proper coverage and complies with government rules. Two representatives were invited for the second evaluation. We shared the artefacts and interview questions with interviewees one week before the interview to allow them to familiarise themselves with the artefacts and questions beforehand.

We started the interview by demonstrating the designed artefacts and design process. We then asked several questions to assess the reasonableness of the artefacts. Each interview lasted about one hour and consisted of three parts (see question list in Appendix A). Part 1 asked about the services provided by their agencies and their understanding of cyber resilience; Part 2 focused on their evaluation of artefacts’ reasonableness and recommendations; Part 3 investigated their knowledge of cyber resilience maturity and experience in measuring continuous improvements for cyber resiliency.

All interviews were recorded and transcribed in full verbatim. All transcripts were also processed manually to rectify errors and then sent to the interviewees to confirm whether they were satisfied with the content or requested changes. We received some interesting feedback during this evaluation.

Feedback 1. “Supply chain management” should be emphasised.

One of our interviewees mentioned that *“this term [supply chain management] does not call out”* (Interviewee 1), although existing practices already include some supply chain management aspects

in “External Dependencies Management”. They argued that the “supply chain management” in current version has not been emphasised properly, and further indicated that organisations place different levels of emphasis on supply chain management when managing external dependencies due to the considerations of organisational attributes, such as size, type, and industry. For some organisations, particularly government agencies, the impact of some risks and vulnerabilities will be shaped by whether they have a good knowledge of suppliers. It is occasionally even required to be thoroughly aware of their providers’ suppliers and other businesses who work with the same supplier. Indeed, the cyber incident at New Zealand government agencies earlier this year confirmed the need for this perspective. A significant amount of private data was leaked from the government public sector and sold on the Dark Web due to a ransomware attack on an organisation that provides IT services to multiple government organisations (Hunt, 2023; Keall, 2023).

Feedback 2. “Human resilience” should be emphasised.

One interviewee stated that most frameworks focus more on technical means to enhance technology to achieve higher cyber resilience. In contrast, human resilience received little attention. Similarly, while some organisations spend a lot of time and money on enhancing systems and acquiring new technologies, *“the capability put in security teams and the capacity put into training the larger organisation on best practices on the use of devices is minimal”* (Interview 2). Therefore, interviewees argued that establishing a “safety culture” is important to enable continuous awareness and improvements.

Feedback 3. Regrouping according to categorisation.

Given that the next round of evaluation will be conducted with interviewers with organisational backgrounds, one interviewer suggested that it might satisfy some users’ preferences by grouping practices according to the categorisation of practices, particularly for users who are clear about their roles and responsibilities in cyber resilience management. The existing (domain-based) grouping enables a step-by-step approach to understanding cyber resilience-related domains and practices. This is helpful for organisations that do not have expertise in this area. Those with related experience might not be interested in the domains and their definitions. The regrouped framework (categorisation-based) allows users to quickly find the areas corresponding to their roles and conduct cyber resilience reviews. By this grouping, the organisation’s people with roles in governance/ operations/ controls can look at the practices that fit their role straightforwardly

without taking the steps of understanding domains and definitions.

Feedback 4. The specificities of the New Zealand business environment should be noted.

The interviewees mentioned that as most organisations in New Zealand are SMEs, many employees do not clearly categorise their roles. For example, for large organisations, the top management level or Board is responsible for leading directions and designing missions, they are rarely involved in daily operations and strategy making. Whereas for an organisation that only contains less than ten people, the roles of management depend on what they are responsible for. Moreover, the difference in responsibilities determines the “hat” they wear for governing or operating. Similarly, organisations’ focus on resource allocation focus varies based on size or industry, meaning they might place a lower priority on some identified vulnerabilities less, or even ignore them on purpose. Moreover, some organisations are hampered by the limited availability of money and resources (people and technology) and do not have specialist personnel on-site. Frameworks or methodologies that contain redundant clauses and sub-categories may not meet their needs and only result in additional time investment and learning costs.

It is worth noting that all interviewees found the practices contained in their current artefacts and categorisations reasonable, which was the baseline criteria that we were assessing the methodology against. They recognised the reasonableness of definitions, practices, and categorisations and agreed that this assisted organisations in correctly understanding cyber resilience and developing direction in an efficient timeframe. However, interviewees generally reflected that merely providing organisations with specific maturity scores was not the key to helping them succeed in improving cyber resilience. The understanding gained through self-assessment of the implemented practices, for example, their strengths and weaknesses, room for improvement, could be one of the possible solutions to improve their cyber resilience.

5.3. Design Cycle of Iteration 3

5.3.1. Designing CRMAM V.03

All feedback was analysed and discussed internally with the research team, and some modifications were made to CRMAM V.02 in response to the analysis. Consequently, we invited employees from 10 commercial organisations to evaluate the artefacts.

In response to the feedback about supply chain management, we generated two reasons for the impression of “*does not call out*” after discussion: Firstly, lack of a clear definition of the scope of “*external dependencies*” in the glossary. We reviewed the related references in whitepapers and academic articles. We found that most frameworks (e.g., CRR, NIST CSF, CERT-RMM) not only provided a detailed definition of “External Dependencies Management” but also stated its scope. These cascading explanations – “External entity” to “External dependencies” to “External dependencies management” – allow users to understand the scope and relevance clearly. In contrast, the lack of such detailed explanations in our artefacts has led to some users, for example, the interviewees in the evaluation, being ambiguous about the subordination between external dependencies management and supply chain management. Secondly, lack of clarity as to what is included in each practice. In the description of the practices in “External Dependencies Management”, we did not indicate the correspondence between the object of each practice and external dependencies. As a result, the user cannot clearly distinguish which practices are generic to all external entities and specific to a particular entity. This ambiguity in the practices’ object led users to overlook external entities that appear less related to organisations’ critical services, such as technology suppliers and infrastructure providers.

In response to the novel idea regarding “human resilience”, we not only reviewed the frameworks again to determine if they made any suggestions for this aspect, but also used the literature review to identify the importance of “human resilience” in the knowledge base. If the reviewed frameworks did not include this aspect that is deemed significant in studies, we still considered its inclusion in our artefacts. During the review of the framework, we found that only CERT-RMM and CRR proposed promoting “a resilience-aware culture” (Caralli et al., 2016, p.195) and developing cyber security awareness activities (CISA, 2020b). Other frameworks paid less attention to this aspect. In contrast, the literature review on “human resilience” and “safety culture” revealed that only a few studies related to cyber resilience focused on the human aspect. Although human mistake is defined as one of the significant causes of cyber incidents in some studies (Hopcraft et al., 2022; Huang et al., 2022; van der Kleij & Leukfeldt, 2020), they did not focus on the function of building a safety culture in improving cyber resilience yet. Among the articles published in recent years, the prominent role of cyber security culture as an often overlooked aspect of the organisational security chain is highlighted increasingly by some academics (Andronache, 2021; Georgiadou et al., 2022). For

example, Georgiadou et al. (2022) suggested that “even the most well-guarded corporation is defenseless with no security culture” (p.452). Therefore, adding practices related to developing a safety culture to CRMAM V.03 might be necessary.

For feedback about “regrouping”, we agreed that a different grouping would assist users in finding a suitable way according to their preferences and thus improve the usability of the artefacts. However, we do not want to limit ourselves to the existing domain-based or categorise-based grouping suggested by interviewees and would instead like to explore more diverse attempts. We conducted a targeted study of the reviewed frameworks to discover additional grouping criteria. We found that “lifecycle” is frequently used as grouping criteria when frameworks providing suggestions, such as NIST CSF (NIST, 2018), Cyber Resilience Matrix (Linkov et al., 2013), and Managerial Cyber Resilience Framework (Annarelli et al., 2020). In the journey of managing cyber resilience, organisations need to operate practices through a continuous, step-by-step process (Azmi et al., 2018). This process involves collecting and analysing information, monitoring vulnerabilities and risks, supporting decision-making, and implementing lessons learned (NIST, 2018). We define this process as a “Cyber resilience lifecycle” (Azmi et al., 2018; NIST, 2018). The “lifecycle” as grouping criteria would provide users with a coherent way of thinking to evaluate the current level of maturity based on existing practices. Therefore, we used “lifecycle” as another grouping criterion when rebuilding CRMAM V.03.

5.3.2. Building CRMAM V.03

After the previous discussion, we had a clearer perception of the evaluators’ feedback and decided how to implement them in the CRMAM V.03. We made improvements in four areas.

Improvement 1. Redefine the scope of “External dependencies”.

To solve the two causes in “External Dependencies Management”, we redefined “External dependencies” more clearly. In our current definition, we defined it mainly based on the definition of “external entity” in CRR: “An individual, business, or business unit that is external to and in a supporting or influencing relationship with organisations” (CISA, 2020, p.48). In CRMAM V.02, we did not describe the scope of “external dependencies” separately, although we have defined it in a similarly broad sense in some practices. For example, we suggested that “[*The organisation should*]

establish and maintain information-sharing and cooperation relationships with external dependencies” (EDM3). This includes not only cooperation with suppliers to monitor potential vulnerabilities and risks during the identify and protect phases, but also to inform clients, partner organisations, internal employees and other affected entities when detecting and responding to incidents. In this case, supply chain management is a sub-section of external dependency management. Therefore, in addition to the current definition, we further explained that the scope of “external dependencies” ranges from individuals (e.g., employees, contractors, and customers) to external organisations (e.g., partner organisations, client organisations, and suppliers).

For the second cause, we distinguished some objects of practice, as shown in Table 9. We added some examples to practices, such as EDM3, where we emphasised that organisations should establish cooperation relationships with clients and partner organisations. Organisations need to maintain sensitivity to the cyber security environment by exchanging information with partner companies. They should also actively exchange the necessary information with clients, especially when a cyber incident happens.

Table 9: Modifications in the EDM domain.

Identify and manage the risks, threats, and vulnerabilities related to external dependencies.	Identify and manage the risks, threats, and vulnerabilities related to external dependencies <u>(especially entities in the supply chain).</u>	EDM2
Establish and maintain information-sharing and cooperation relationships with external dependencies.	Establish and maintain information-sharing and cooperation relationships with <u>clients, partner organisations, and other</u> external dependencies.	EDM3
Communicate to external dependencies to clarify roles and responsibilities.	Communicate to external dependencies <u>(e.g., contractors, clients, partner organisations, suppliers)</u> to clarify roles and responsibilities.	EDM4

Improvement 2. Add new practice about “Human Resilience”.

Another change is adding practices related to “Human Resilience” in “Training and Awareness”. After

reviewing the frameworks and literature, we added a new practice to CRMAM V.03 in conjunction with CERT-RMM's practice on human resilience: *"Build a resilience-aware and -ready culture in multiple ways"* (TA5). As proposed in CERT-RMM, organisations should create a safe environment for employees to develop an awareness of resilience and a resilience-ready culture (Caralli et al., 2016). There are many means to achieve this goal, such as establishing recognition mechanisms to reward employees for maintaining operational resilience, providing opportunities for employees to talk freely about resilience, and supporting the implementation of resilience-related policies (Georgiadou et al., 2022; Zwilling et al., 2022).

Improvement 3. Add new criteria for grouping practices.

We considered regrouping the practices by three criteria: domain (Figure 8), categorisation (Figure 9), and lifecycle (Figure 10). To do this, we added a new list of practices named "function". The "function" denotes one of the phases of the cyber resilience lifecycle that each practice corresponds to. The lifecycle comprises 5 phases: Identify, Protect, Detect, Respond, and Recover (NIST, 2018). We added practices' functions by considering the suggestions in the reviewed frameworks, especially CRR, NIST CSF, then grouped each practice based on their functions. After two rounds of reviewing and checking, we regrouped all practices by their function, category, and domain, resulting in three versions (Figure 8; Figure 9; Figure 10). All three versions contained the same amount of information and were grouped according to different criteria. To maintain consistency of practice, the code (see code example in Figure 5) of each practice remained the same in three versions.

Domain	Definition	Code	Function	Categories	Practices	Sub-categories				CRR
						Name	Yes	No	Not sure	
Asset management (AM)	It refers to the actions the organisation takes to identify, record and manage the organisation's critical assets.	AM1	IDENTIFY	Operation	Identify and maintain physical, software and information assets inventory with specific details.	People				AM.G2
						Process				AM.G3
						Technology				AM.G4
						Information				AM.G7
		AM2	IDENTIFY	Operation	Prioritise assets based on their business value, classification, and criticality.	People				AM.G1
						Process				
						Technology				AM.G7
						Information				
		AM3	IDENTIFY	Operation	Identify and record the assets related to key critical services.	People				AM.G1
						Process				
						Technology				AM.G2
						Information				
		AM4	PROTECT	Control	Create information confidentiality, integrity, availability (CIA) checking mechanism.	People				CCM.G2
						Process				
						Technology				CM.G2
						Information				
AM5	PROTECT	Control	Implement measures to protect, backup, and maintain information assets and related activities (e.g., data-at-rest; data-in-transit; data leaks).	People				AM.G6		
				Process				CM.G2		
				Technology				CCM.G1		
				Information						
Controls management (CM)	Control management aims to improve the security of critical services by identifying, analysing, and managing the operational environment. Controls management focuses on the control of any factors that may affect the	CM1	PROTECT	Operation	Define control objectives and design a control plan.	People				CM.G1
						Process				
						Technology				CM.G3
						Information				
		CM2	PROTECT	Operation	Establish identities and manage authentication.	People				AM.G5
						Process				
						Technology				
						Information				
		CM3	PROTECT	Operation	Manage physical access to critical assets/services.	People				AM.G5
						Process				CM.G2
						Technology				CCM.G1
						Information				

< >

Version1.domains

Version2.categories

Version3.lifecycle

Reference sheet

Glos ...

+

:

Figure 8: Group by domains [Version 1].

Categories	Definition	Code	Function	Domain	Practices	Sub-categories				CRR
						Name	Yes	No	Not sure	
Governance	The processes that identify the key business services and business activities to evaluate risk and maturity and allocate priority for guiding operations about the focus areas.	GO1	IDENTIFY	Governance	Identify and prioritise key critical services, business missions and objectives.	People				AM.G1
						Process				
						Technology				AM.G2
						Information				
		GO2	IDENTIFY	Governance	Develop a cyber resilience plan and clarify roles and responsibilities.	People				CM.G2
						Process				
						Technology				
						Information				
		GO3	IDENTIFY	Governance	Establish a set of relevant internal and external guidelines, policies and other obligations.	People				CM.G2
						Process				
						Technology				AM.G7
						Information				
		VM2	IDENTIFY	Vulnerability management	Identify potential business impacts and likelihoods of each threat and vulnerability.	People				VM.G2
						Process				
						Technology				RM.G4
						Information				
		RM1	IDENTIFY	Risk management	Develop a strategy for identifying, analysing, and mitigating risks.	People				RM.G1
						Process				
						Technology				
						Information				
		EDM1	IDENTIFY	External dependencies management	Identify and prioritised external dependencies based on their function.	People				EDM.G1
						Process				
						Technology				EDM.G5
						Information				
		EDM2	IDENTIFY	External dependencies management	Identify and manage the risks, threats, and vulnerabilities related to external dependencies (especially entities in the supply chain).	People				EDG.G2
						Process				
						Technology				
						Information				
		EDM3	IDENTIFY	External dependencies	Establish and maintain information-sharing and cooperation relationships with clients, partner organisations, and other external dependencies.	People				EDM.G3
						Process				
						Technology				

Figure 9: Group by categorisation [Version 2].

Function	Definition	Code	Domain	Categories	Practices	Sub-categories				CRR	
						Name	Yes	No	Not sure		
IDENTIFY	Develop an organisational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.	AM1	Asset management	Operation	Identify and maintain physical, software and information assets inventory with specific details.	People				AM.G2	AS
						Process				AM.G3	
						Technology				AM.G4	
						Information				AM.G7	AS
										AM.G6	
		AM2	Asset management	Operation	Prioritise assets based on their business value, classification, and criticality.	People				AM.G1	A
						Process					
						Technology				AM.G7	
						Information					A
		AM3	Asset management	Operation	Identify and record the assets related to key critical services.	People				AM.G1	AS
						Process					
						Technology				AM.G2	
						Information					
		GO1	Governance	Governance	Identify and prioritise key critical services, business missions and objectives.	People				AM.G1	AS
						Process					
						Technology				AM.G2	
						Information					
		GO2	Governance	Governance	Develop a cyber resilience plan and clarify roles and responsibilities.	People				CM.G2	ARCI
						Process					PE
						Technology					PE
						Information					
		GO3	Governance	Governance	Establish a set of relevant internal and external guidelines, policies and other obligations.	People				CM.G2	PE
						Process					
						Technology				AM.G7	PE
						Information					
		VM1	Vulnerability management	Operation	Identify the organisation's vulnerabilities (internal and external) and repeat the procedure periodically.	People				VM.G2	T
						Process				VM.G3	
						Technology				VM.G1	
						Information					
		VM2	Vulnerability management	Governance	Identify potential business impacts and likelihoods of each threat and vulnerability.	People				VM.G2	T
						Process					
						Technology				RM.G4	
						Information					

Figure 10: Group by lifecycle [Version 3].

Improvement 4. Add subcategories and a reference sheet.

To improve the usefulness of artefacts, we added subcategories to CRMAM V.03. This allows organisations to compare and assess the subcategories of each practice to clarify their maturity among different assets. Most reviewed frameworks mentioned that organisations normally contain four assets: people, process, information, and technology (Caralli et al., 2016; NIST, 2018). Some frameworks considered facility as another type of asset (CISA, 2020b). In our methodology, we considered technology and facility in the same category because they can both be considered as the infrastructure of organisations that support business activities. Organisations need to implement protection for these four assets and evaluate their practices' performance (CISA, 2020b; Linkov et al., 2013). Therefore, we added the subcategories: People, Process, Information, and Technology. To maintain consistency, each practice contains four subcategories. Each subcategory contains three options: Yes, No, Not Sure. Organisations can choose the appropriate option to define their status. To avoid inconsistent interpretations by users with different levels of expertise, we created a reference sheet (see Figure 11) to explain the meaning of the subcategories in each practice. By answering questions in the reference sheet, organisations can better understand cyber resilience and their position of maturity (you can find the full version of CRMAM V.03 here <https://osf.io/q7gpx/files/osfstorage/649bd3c73809110ca53c3257>).

Code	Practices	Sub-categories				
		Name	Question	Yes	No	Not sure
AM1	Identify and maintain physical, software and information assets inventory with specific details	People	Are people assets (human resources) inventory identified and maintained periodically with specific details?			
		Process	Are process related assets inventory identified and maintained periodically with specific details?			
		Technology	Are technology assets inventory identified and maintained periodically with specific details (technology includes hardware, software, and external information systems)?			
		Information	Are information assets inventory identified and maintained periodically with specific details?			
AM2	Prioritise asset based on its business value, classification, criticality	People	Are people related assets prioritised based on their business value, classification, and criticality?			
		Process	Are process related assets prioritised based on their business value, classification, and criticality?			
		Technology	Are technology related assets prioritised based on their business value, classification, and criticality?			
		Information	Are information related assets prioritised based on their business value, classification, and criticality?			
AM3	Identify and archive the assets related to key critical services	People	Are people assets related to key critical services identified and recorded?			
		Process	Are process assets related to key critical services identified and recorded?			
		Technology	Are technology assets related to key critical services identified and recorded?			
		Information	Are information assets related to key critical services identified and recorded?			
AM4	Create information confidentiality, integrity, availability (CIA) checking mechanism	People	Are CIA requirements used to determine which people are authorised to maintain information assets?			
		Process	Has a process for creating and managing the CIA checking mechanism been implemented?			
		Technology	Are technologies in use to support the CIA checking mechanism?			
		Information	Is the CIA checking mechanism performed for information assets?			
AM5	Implement measures to protect, backup, and maintain information assets and related activities (e.g., protect data-at-rest, data-in-transit; monitor data leaks)	People	Are all staff who handle information assets trained in the use of information?			
		Process	Have controls been implemented to protect, back up, and maintain information assets?			
		Technology	Have technologies been implemented to protect, back up, and maintain information assets and related activities?			
		Information	Are information assets protected, backed up, and maintained?			

Figure 11: Reference sheet for sub-categories (partially).

5.3.3. Evaluating CRMAM V.03

After completing the improvements, we contacted and recruited some employees responsible for cyber security in commercial organisations to evaluate CRMAM V.03. This approach was based on their commercial work experience and ability to test the reasonableness and functionalities of CRMAM in organisational environments. All interviewees are required to have a certain level of expertise in cyber security or cyber resilience and organisational work experience. Their attributes are shown in Appendix C. Organisation size is defined by the criteria used in the New Zealand government document (MBIE, 2019; Roberts, 2021); the “small organisation” in this standard refers to organisations with fewer than 20 employees instead of fewer than 50 employees in many countries.

We contacted them one week before the interview to share artefacts and asked them to familiarise themselves with CRMAM V.03. We also emphasised in recruitment information that they are welcome to try the methodology in their business environment or to invite other appropriate colleagues to research it. After that, we conducted one-on-one interviews. Like the previous evaluations, each interview was recorded, transcribed into text, and sent to the interviewee afterwards to confirm the content. Each interview lasted approximately one hour. We added some questions to the interview agenda used in the second evaluation (see question list in Appendix B). These new questions covered three areas: 1) Understanding organisations’ structure regarding cyber resilience or cyber security and how they reacted and recovered from cyber incidents; 2) Asking the reasonableness of artefacts and their preferences on the different groupings and subcategories; and 3) Understanding whether organisations understand their cyber resilience maturity and how to measure and manage continuous improvements.

After completing interviews with all respondents, we gathered valuable feedback. All interviewees agreed on the reasonableness and functionalities of the methodology, which meets the baseline of this round of evaluation, while some improvements are provided. They all agreed that the methodology allows the user to gain the understanding of cyber resilience quickly and correctly. We used NVivo to code all transcriptions and divided their feedback into three categories according to their importance (see Table 10). We noticed that the feedback from interviewees is diverse and comes from different entry points and focuses. It might be because all interviewees have years of

experience working in organisations and have some insights into designing cyber resiliency tools. Their feedback combined the pain points from using other resiliency frameworks, such as lack of toolkits and instantiations. Some feedback seemed highly influenced by their personal view of dealing with cyber resiliency. Therefore, it would be unwise to implement all feedback into artefacts based on an individual view only. We grouped the feedback according to its relevance and importance to CRMAM. Each category is introduced in detail below.

Table 10: Feedback grouped by importance.

Essential for design objectives
1. [Relation map] The three categories' interfaces were not reflected.
2. [Relation map] It did not show how lessons learned from operations and controls be fed back to governance.
3. [Framework] It would be helpful to show the linkages and sequences between domains and practices.
4. [Framework] Lack of emphasis on ownership and accountability for cyber security.
5. [Sub-categorisation] Sub-categories are redundant compared to categorisation and lead to confusion.
6. [Framework] Lack of expression of the result.
7. [Framework] NZISM is not included in the reviewed frameworks.
Nice-to-have for future work
8. [Framework] Need a toolkit and examples for categorisations and practices.
9. [Versions] Design a software-based tool to populate the suitable version according to their answer and add helper text for each practice.
Good idea but out of scope
10. [Categories] Expect more suggestions on controls.
11. [Relation map] Have representations of how risks fit into categorisations.
12. [Categories] Use people, process, and technology as categories.

5.3.3.1. Essential for Design Objectives.

For the feedback mentioned by most people and is highly related to artefacts, we listed them with higher priority and grouped them as "Essential" (see Table 11). This type of feedback should be

adopted into CRMAM as they are closely associated with the design objectives and aid in improving the artefacts to become a suitable tool for the target audience.

Table 11: Feedback that is essential for design objectives.

Essential for design objectives	
1.	[Relation map] The three categories' interfaces were not reflected.
2.	[Relation map] It did not show how lessons learned from operations and controls be fed back to governance.
3.	[Framework] It would be helpful to show the linkages and sequences between domains and practices.
4.	[Framework] Lack of expression of the result.
5.	[Framework] Lack of emphasis on ownership and accountability for cyber security.
6.	[Sub-categorisation] Sub-categories are redundant compared to categorisation and lead to confusion.
7.	[Framework] NZISM is not included in the reviewed frameworks.

Feedback 1. Lack of interfaces between categories.

Some interviewees suggested that the existing relationship map for the three categories did not reflect their interfaces. These categories should be independent but also have overlapping and collaborative connections. They emphasised that since most New Zealand organisations are SMEs, it is not always possible for a small organisation to have those three things separately (Interviewee J). Often in organisations, the staff who govern and set the direction are the people who develop specific strategies based on the direction and implement them (Interviewees C and I). In this case, governance and operations are performed by the same group, even the same individual (Benz & Chatterjee, 2020; Carías et al., 2021). Similarly, in the medium-sized and large organisations interviewed, the interviewees (Interviewee A) emphasised that despite the clear separations among performers of three categories, they tend to work collaboratively or even perform multiple roles simultaneously most times. In other words, organisations believe that when strategy development and implementation are executed by the same group of employees, it is conducive to understanding strategies accurately and making actionable adjustments. Interestingly, although some employees could not clearly define their roles because of the blurred boundaries between the three in a real-world workplace, their performance was not affected as long as they had a specific focus on their

workload (Interviewee A).

This blurred boundary is also present in resource allocation and management. In the current relationship map, we assigned assets to three categorisations and showed how organisations manage them accordingly. Some interviewees emphasised that in real-world environments, it is challenging to distinguish assets as such based on how they are used. In “production”, assets allocated at controls are not just technology. It also requires the cooperation of people and processes. Therefore, the current relationship map is misleading in this regard.

Feedback 2. Not show how the lesson was learned feedback to upper levels.

Some interviewees suggested that “governance – operations – controls” is not a one-way street. Problems and lessons that arise in controls and operations should also be fed back into governance (Interviewees H, I). In the current relationship map, we only emphasised the role of governance in guiding operations and controls and the role of operations in managing controls. However, we neglected that controls – as the infrastructure for implementing practices and the front line for facing cyber threats – can gain many experiences from practices and cyber incidents. These experiences can be meaningful for organisations to evaluate implemented practices and adjust resources. Meanwhile, operations also need to filter the feedback gained from controls and pass it to governance to assist top management in determining the appropriateness of direction and making subsequent instructions.

Feedback 3. Lack of linkages and sequences between domains and practices.

Some interviewees suggested that it would be helpful to show the linkage and sequence between domains and practices (Interviewees C, B). They argued that although we provided multiple versions of CRMAM V.03, which assisted organisations in quickly finding specific practices based on their roles, some organisations that are new to the cyber resilience management journey are often unable to assess their maturity in the correct order. This potentially causes some disruptions to their assessment process. In CRMAM V.03, we did not explicitly indicate the order of practices. Therefore, we find this suggestion to be valuable.

Feedback 4. Lack of emphasis on ownership and accountability

One interviewee (Interviewee E) pointed out that the emphasis on ownership and accountability for

cyber security is not evident in existing practices. They believed “It is dangerous when employees are unclear about their roles and responsibilities in cyber resilience” (Interviewee E). In this case, even though organisations have appropriate plans in place, employees cannot execute these plans, especially when cyber incidents occur. Furthermore, ownership and accountability are essential in preparing and responding to an incident. Although most cyber incidents are caused by careless behaviours in a phishing email, the impact and manifestations of cyber incidents are significant and varied. Therefore, organisations should also set practices regarding appointing specific leaders to assign and adjust ownership to respond to the changes during cyber incidents.

Feedback 5. Redundant on sub-categories

While some agreed that the subcategories and reference sheet assist organisations in reducing misinterpretations, especially when reviews are rolled out by collaboration of multiple employees, some interviewees raised concerns. They expressed concerns on two aspects. Firstly, they argued that this subcategory would add another layer of complexity, which goes against the design objective of reducing the complexity of professional frameworks. Some interviewees claimed that their first reaction to the reference sheet (about 150 questions) was that “there are too many questions that required thoughtful consideration to answer” (Interviewees H, I). Secondly, one interviewee (Interviewee G) with many years of experience questioned the need for having categories and subcategories simultaneously. They suggested that adding subcategories can potentially cause confusion and disturbance to organisations, therefore should be removed. Interviewees who positively responded to the subcategories also illustrated that some subcategories are inappropriate for practices and should be greyed out; they believed that the current sub-categories are redundant.

Feedback 6. Lack of expression of results.

One interviewee (Interviewee J) was confused about the assessment results' presentation after using CRMAM. They argued that although CRMAM V.03 provides three options (Yes, No, Not Sure) as criteria for organisations selecting, there are two problems with this representation. Firstly, these three options are too restrictive. For organisations that may begin their journey in cyber resiliency management, it is difficult for them to describe where they are with current options accurately. For example, organisations can determine if they have a practice related to “creating cyber resiliency plans”, but they cannot choose the exact answer to describe the status if this plan is still in the designing process and fully completed. Secondly, even if organisations had completed the review,

they did not have expressions about accurately positioning their maturity through the review results. In other words, they need further assistance in making sense of the results gained from the methodology.

Feedback 7. NZISM is not in the reviewed frameworks.

During the interviews, we also noted that most organisations use NIST CSF, ISO 27001, CERT-RMM, and New Zealand Information Security Manual (NZISM) as the basis for their practices. However, when we designed CRMAM, our reviewed framework did not cover NZISM. NZISM is designed by New Zealand government agencies and has been widely used by commercial organisations in New Zealand (NCSC, 2020). The neglect of NZISM leads us to question the coverage of CRMAM against the New Zealand organisational environment.

5.3.3.2. Nice-to-have for Future Work.

The feedback that is beneficial for improving user experience was grouped as “Nice-to-have” (see Table 12). The current study might not be able to implement them as they are time-consuming and may not essentially meet our design objectives. This feedback is considered as bonus features in future work.

Table 12: Feedback that nice-to-have.

Nice-to-have for future work
8. [Framework] Need a toolkit and examples for categorisations and practices.
9. [Versions] Design a software-based tool to populate the suitable version according to their answer and add helper text for each practice.

Feedback 8. Need a toolkit and examples.

As mentioned before, most professional frameworks contained many supplementary materials. Some interviewees suggested that CRMAM should also provide a toolkit to explain how to use it sensibly and provide examples of practices (Interviewees G, H). One interviewee (Interviewee J) suggested further that the methodology should provide a way to allow organisations to describe their cyber resilience maturity in two states: the current state and the target state. The current state refers to the maturity level generated by CRMAM to evaluate the organisation’s implemented

practices, and the target state refers to the maturity level that the organisation would like to achieve in the future. Each state contains factors such as capability, capability coverage, and maturity. In this way, organisations can set up their goals and roadmap after using them. Similarly, another interviewee (Interviewee I) suggested providing examples for each component of the relationship map to describe associated activities specifically. Although the relationship map shows how they work together to support business activities, some real-world examples could be helpful for organisations from different backgrounds.

Feedback 9. Create a software-based tool.

Most interviewees mentioned the limitations of Excel-based tools (Interviewees E, D). Since most of them have backgrounds in computer science, they agreed that creating software-based tool is a better means to design methodology. Specifically, when we introduced three groupings, one interviewee (Interviewee D) suggested adding a pre-step survey to collect the user's basic information (e.g., position, background, familiarity with professional frameworks). After analysing collected information by some algorithms, the methodology can populate the appropriate version of grouping and provides the option to show methodology in the way that suits them. Similarly, the examples of practices suggested in the previous feedback can be added as helper texts. This provides support for those who need assistance and reduces the concern of complexity.

5.3.3.3. Good Idea but Out of Scope.

The feedback with clear personal preferences and user habits was categorised as a "Good idea" with the lowest importance (see Table 13). As these suggestions did not align with the focus of our study, we only discussed why they were defined as out of scope and not to be implemented.

Table 13: Feedback that is a good idea but out of scope.

Good idea but out of scope.
10. [Categories] Expect more practices on controls.
13. [Relation map] Have representations of how risks fit into categorisations.
11. [Categories] Use people, process, and technology as categories.

Feedback 10. Expect more control-related practices.

One interviewee (Interviewee G) argued that controls are the fundamental part of cyber resilience management and “resilience is heavily weighted around controls and operations, and then some checks and balances of governing” (Interviewee G). In other words, they think CRMAM V.03 did not contain enough control-related practices. As we mentioned, most frameworks focused on providing advice on controls and technical support. This somewhat contributes to the misconception – some organisations are overly focused on controls and technology adoption at the expense of adjusting processes and training staff to work with the new technologies – and ultimately leads to a failure of cyber resiliency management. In the previous evaluation, one of the interviewees (Interviewee 2) from a government agency also mentioned that thoughtlessly and quickly adopting emerging technologies to follow trends may create a lack of adaptation between employees and technology that causes more significant risks and threats. “How to drive a car safely” is a question for every organisation that “keeps buying new cars” to drive on the cyber resilience journey. Therefore, this study does not focus on providing specific control methods. Instead, it aims to provide them with directions to understand maturity status from a high-level view. We tend to provide a simplified review methodology that assists organisations in achieving their assessment.

Feedback 11. Have representations of risks in categorisation.

One interviewee (Interviewee C) believed that cyber resilience management is inherently risk-driven and suggested emphasising the influence of risk in categorisations by visual representation. However, based on our observations during interviews, most organisations have different structures for cyber resilience management. Some interviewees from SMEs mentioned that they do not distinguish between governance and operations for cyber resilience, while some organisations, especially large multinationals, establish another level of managers between operations and governance to manage the organisation’s local branch. To provide a proper picture of the relationship between risks and categorisations in different organisations, it is necessary not only to analyse organisational structure through a systematic study of the knowledge base but also to collect data related to organisations. This is inconsistent with this study’s goal of providing a maturity assessment solution, so we believe this is beyond the study’s scope.

Feedback 12. Use people, process, and technology as categories.

One interviewee (Interviewee B) suggested using people, process, and technology as categories for group practices. They believed this categorisation aligns with how some cyber security companies

conduct inspections. In fact, this idea has been tested when redesigning CRMAM V.02. When the evaluator from the first evaluation suggested categorising practices, we attempted to categorise them based on “people, process, technology” as well. However, we found that most practices required organisations to mobilise all three assets simultaneously to achieve the desired results. It was not easy to define the categories by the assets used in practices. However, we acknowledged the interviewee’s feedback that this categorisation is familiar to organisations and might be helpful in assessment. Therefore, we also added an explanation in the methodology to emphasise the need to assess practices considering four assets (people, process, technology, and information).

5.4. Design Cycle of Iteration 4

5.4.1. Designing CRMAM v.04

Based on the importance grouping in the previews step, we focused on implementing the feedback classified as “Essential to meet objectives” in this iteration, as they are more in line with design objectives. Each feedback in this category was studied and analysed, and the methodology was adjusted accordingly. The feedback grouped as “Nice-to-have” is discussed in the future study section as a way to enhance the methodology in the future.

1. Redesign the relation map.

We reviewed the types of categorisations and assets in organisations and found that there are indeed ambiguities in the current relationship map. According to the current map, “management” refers to performers from the middle management of organisations, such as department managers. However, for organisations with insufficient size or capabilities to segment their people in this way, people who work in governance and operations are often mixed and even the same person (Benz & Chatterjee, 2020; Carías et al., 2021). Therefore, interviewees found this representation to be incompatible with their work environment. We decided to redesign the relationship map by adopting one interviewee’s suggestion: using a Venn diagram to represent the interfaces between categorisations and assets.

In addition, regarding “show operations and controls fed back to governance” (Interview H), we also found this as a shortage in the current map. Since we used a flow chart to represent how products

are accomplished using assets under the collaboration of three categorisations, this somehow implies their independent relationship, which does not accurately describe how organisations orchestrate them as an ecosystem. This is why interviewees complained that it failed to accurately portray the impact of controls on the counter-push of the higher categories. Thus, this feedback should also be represented in the new relationship map.

2. Show linkages and sequences between domains and practices.

We reviewed the frameworks again based on the feedback regarding the linkages between domains and practices. We found that most of them did not clearly describe the sequence of suggestions (Caralli et al., 2016; CISA, 2020b). Although NIST CSF used functions (Identify, Protect, Detect, Respond, and Recover) to group suggestions (NIST, 2018), we did not consider this to be a sequential relationship as “function” is for domains rather than individual practices. Although no evidence was found in the professional frameworks to justify the importance of having sequential order for practices, this might be one of their disadvantages: not meeting the demands of organisations. This feedback has practical considerations and should be implemented into the methodology.

3. Delete subcategories.

We conducted a group discussion in response to the feedback about subcategories. Firstly, we re-examined the subcategories considering design objectives. As we emphasised, the high complexity of the professional frameworks is one of the reasons why organisations cannot use them accurately (Alahmari & Duncan, 2021; Li et al., 2019), especially for SMEs that do not have sufficient capabilities (Benz & Chatterjee, 2020; van Haastrecht et al., 2021). This represents the size of most New Zealand organisations. We must reduce the complexity of the methodology to lower the barriers to use. Secondly, we re-examined the reviewed frameworks. Although these frameworks emphasised that organisations should execute practices with the consideration of subcategories, they more often included these subcategories in explanatory text rather than put them in actual practices (CISA, 2020b; Muneer, 2022). Given that most interviewees questioned the need for subcategories, which caused more confusion, we removed them from the methodology and only emphasised them in supplemental materials such as the reviewed frameworks have done.

4. Add a new method for expressing results.

For the two issues raised by interviewees about result expressions, we agreed that “the available

options are too extreme". In fact, after the last evaluation, to verify if organisations could make decisions for the next step based on CRMAM's result, we simulated the assessment process by using the publicly available information of an SME in New Zealand. This organisation was chosen for two reasons: its size represents most New Zealand organisations, and it is one where we could find the most detailed information. We acted as reviewers to assess their practices based on the information obtained. If there is clear information to prove that a specific practice was implemented, we marked it as "Yes". If no clear information could be found as evidence, the marker was "Not Sure". We found that it was not easy to judge the practice's status by these three options, and maturity could not be visualised clearly with a set of scattered data. Therefore, it is necessary to add more options to describe status accurately and to consider a more intuitive presentation of the results.

5. Emphasise ownership and accountability.

We did a literature review to analyse this feedback. Firstly, the reviewed frameworks have considerations about the importance of assigning ownership and responsibility to cyber resilience. CRR mentioned "roles and responsibilities" in several domains and claimed that organisations should clarify the responsibilities of employees, assets, and stakeholders (CISA, 2020b). NIST CSF also suggested that organisations communicate their roles and responsibilities to participants (NIST, 2018). C2M2 and CERT-RMM emphasised "Assign responsibility, accountability, and authority" as a generic goal in every domain (Caralli et al., 2016; Muneer, 2022). After that, we conducted a review of academic articles. Compared to the emphasis on "communicate roles and responsibilities" in the reviewed frameworks, academics focused more on the impact of "accountability". For example, van de Poel (2020) argued that organisations need to maintain a certain level of transparency and traceability of decisions in cyber security practices to safeguard consumers' data storage security. Alqahtani and Braun (2021) also suggested that accountability is critical to ensuring employees accomplish their tasks promptly. Thus, by combining the findings from frameworks and literature, this component should be made more explicit in some practices.

6. Investigate NZISM

Given that most interviewees stated that their organisations use NZISM as a guideline, which was not included in our reviewed frameworks, we conducted a study of NZISM to determine its relevance to our methodology. NZISM is a manual for information security protection (NCSC, 2020). It classified categories of information and identified all roles and responsibilities related to information security

(NCSC, 2020). Although it mentioned incident management and risk management with some details, the entire manual focused on the secure collecting, using, and archiving of information. In contrast, we aim to design a methodology that covers a broader area than just information security. Cyber resilience management should not only focus on protecting information assets but should also allocate attention to people, processes, and other aspects. Thus, to some extent, CRMAM V.03 included the practices proposed by NZISM. Information management in CRMAM is dispersed across multiple domains. This does not mean it is considered less important. On the contrary, this aspect is critical and should be considered in scenarios by combining it with practices across domains. However, it is undeniable that NZISM is far superior to CRMAM regarding the level of detail and coverage of information security-focused practices. NZISM could be a reference when assessing organisations' cyber resilience and executing practices within operations and controls space.

Furthermore, we made some speculations about possible reasons why NZISM was not raised in the previous evaluations. Firstly, the evaluators in the second round are representatives from government agencies. We asked questions about the frameworks they had used in the "cyber resilience journey". Since NZISM is more concerned about information protection than cyber resilience, they might not have considered this framework to be one of the "cyber resilience frameworks". Another reason might be that most of their answers centred on the "cyber security frameworks" they used in the work environment. The NZISM might not be included in this context. To some extent, this also reflects the unpopularity of cyber resilience frameworks and the limitations of people's understanding of cyber resilience management.

5.4.2. Building CRMAM V.04

After analysing, we made three improvements to CRMAM: redesigned the relationship map to show categorisations' interfaces, created a colour system to show the sequence between practices, and designed new representations to assist organisations in understanding the assessment results.

Improvement 1. Redesign relationship map

We redesigned the relationship map in response to the first two suggestions (see Figure 12). The new relationship map consists of three parts. Firstly, we used a Venn diagram to represent the relationships between governance, operations, and controls. As the interviewees said, organisations

need all three to work together to achieve their goals in business activities most of the time. Although the functions of the three categories are separated in some large organisations, they are interconnected and communicated consequently (Kosutic & Pigni, 2022; van Haastrecht et al., 2021).

Secondly, we added the three aspects that organisations need to consider in the overlapping areas. Each categorisation contains three assets. Organisations need the cooperation of employees to translate the Board's direction into actionable strategies (Iovan & Iovan, 2016; Musa, 2018). In operating environments, governance and operations share people and processes to enable effective cooperation (van Haastrecht et al., 2021). Employees at operations need support from controls to implement the strategies into specific processes and facilities. Their usage of assets is shifted slightly according to their roles. Governance relies more on the people aspect to provide high-level guidance and make decisions. Operations focus on how to maintain activities in specific processes. Controls rely on technology, equipment, and other infrastructures to achieve goals. This is also evident in the overlapping components.

Finally, the third part is the arrows that surround each categorisation. They represent the process of mutual guidance and feedback between the three categorisations. Governance has varying degrees of guidance to operations and controls but also receives feedback from controls and operations. Controls can also pass on the lessons learned, and information gathered to operations for analysis and communication to governance. Organisations can deliver products and services efficiently, safely, and sustainably when these elements work together.

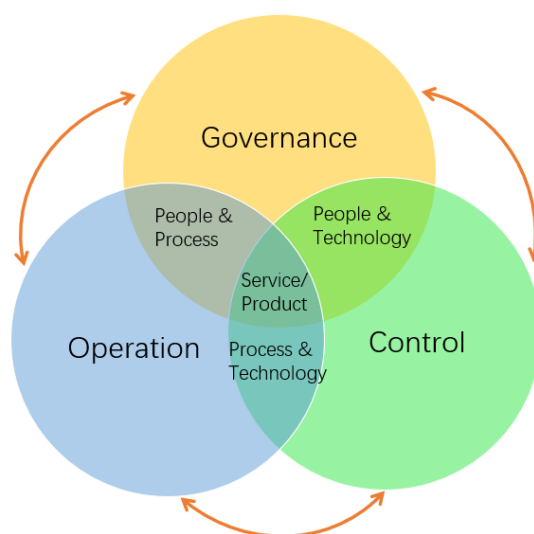


Figure 12: Redesigned relationship map

Improvement 2. Add a colour system to practices.

In response to this feedback, we added a colour system to the practices. Firstly, we rechecked each practice's order using NIST CSF as the standard. We chose this framework for two reasons: 1) It is actively used by governments and organisations worldwide and was mentioned by all interviewees; 2) The supplemental materials related to NIST CSF, including the crosswalk with references to NIST CSF, CRR, ISO27001, CERT-RMM and other frameworks (Homeland Security, 2014), which provide support in mapping these frameworks accurately. After that, we placed practices that could be reviewed simultaneously closely and marked them with the same colour. During our examination, we found that some practices are related even though they do not belong to the same domain. So, we used a similar colour to represent them. We used the following example (Table 14) to explain this process.

Table 14: Example of the colour system.

AM1: Identify and maintain physical, software and information assets inventory with specific details.
CO1: Identify and prioritise key critical services, business missions and objectives.
AM2: Prioritise assets based on their business value, classification, and criticality.
AM3: Identify and archive the assets related to key critical services.
CM1: Establish asset configuration baseline.

In Asset Management, organisations should first create asset inventories and include specific details. Meanwhile, when identifying assets, organisations should clarify their business missions and critical services (CISA, 2016a). So, these two practices (AM1, CO1) are labelled using the same colour. The practices related to analysing, prioritising, and archiving assets should be performed after identifying them and establishing the asset inventory (CISA, 2016a, 2020b). We labelled AM2 and AM3 using a deeper colour. Finally, organisations should establish an asset configuration baseline to record all aspects and create a security template for future changes (Knapp, 2011). This series of practices is interlocking and interconnected. Therefore, we set them in a similar colour but with different degrees of darkness to distinguish their order of precedence.

Improvement 3. Add a new method for expressing results.

To add appropriate presentations, we did some related investigations. Firstly, for the selectable options (Yes, No, Not sure), we examined the solutions offered in the knowledge base. One of the most popular solutions is the five-point Likert scale rating system for maturity level assessment (Tiong Tan et al., 2021; Yigit Ozkan, 2022). Some studies also used specific factors as criteria to measure maturity, such as people capability (Curtis et al., 2009). However, these measures share a common problem: they require additional explanations to allow users to use them properly. Such complex measures add another layer of complexity to the methodology. Therefore, we decided to only add one new criterion – “In progress” – to the existing criterion to refer to those practices that are in design and not finished yet.

In addition, we designed two conceptualisations regarding the presentation of the results. Firstly, organisations obtain a dataset of each practice’s selected options after reviewing. Their maturity is determined by the frequency of selected options – more “Yes” means higher maturity. Secondly, on top of this, we used a diagram to represent the maturity of each practice and the status of these practices in the lifecycle (the left diagram in Figure 13). Each practice corresponds to a spot in this diagram. Each categorisation (Governance, Operations, Controls) corresponds to a coloured line. Organisations can use them to link the practice’s status by their categories (the right diagram in Figure 13). This diagram is divided into five parts according to practices’ functions. Functions that contain more practices occupy a larger area. This approach allows organisations to observe the status of practices and which categories are weak based on the corresponding lines.

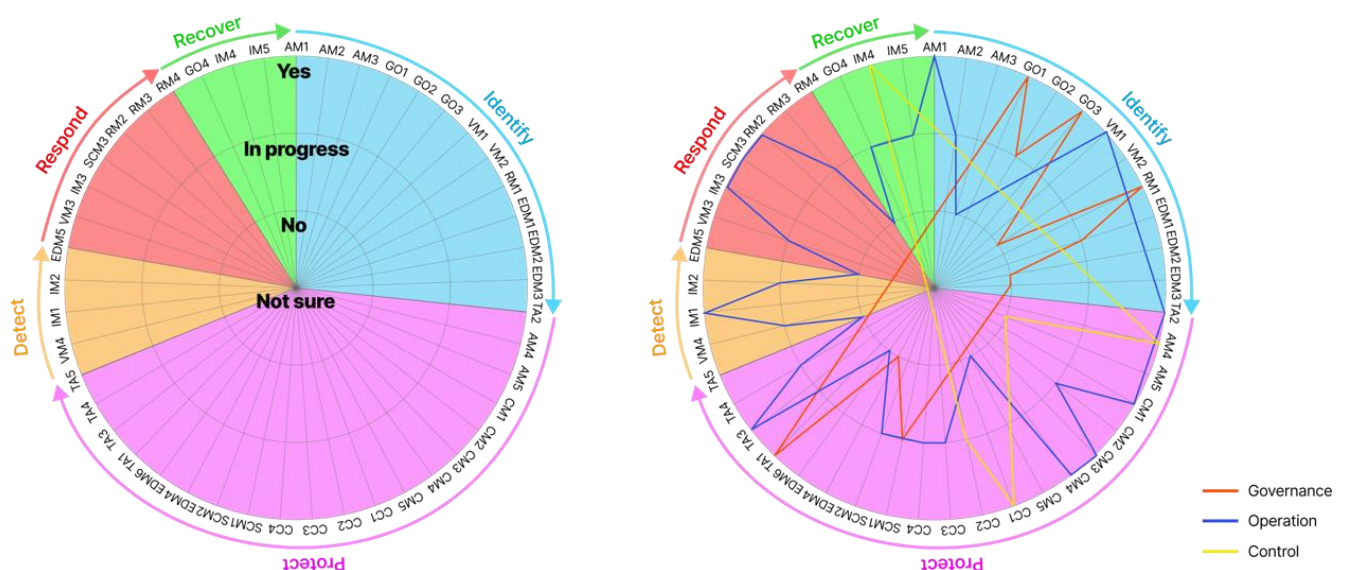


Figure 13: Graphical expression of CRMAM result.

Improvement 4. Emphasise ownership and accountability.

As discussed above, we decided to rewrite the description of practices in the “Governance” domain. In GO2, we emphasised the need for organisations to have a proper cyber resilience plan in place. This plan needs to include details about defining the roles and responsibilities of individuals and people involved, and assigning ownerships and accountabilities for cyber security (Jensen, 2019; van de Poel, 2020). Especially when reacting to cyber incidents, the employees should clarify their responsibilities and how to execute the incident response plan to reduce the damage and recover from it on time.

After these improvements, the CRMAM V.04 is shown below in Figure 14 (you can find the full version of CRMAM V.04 here <https://osf.io/q7gpx/files/osfstorage/649bd3d56c09810c637d20b0>).

Domain	Definition	Code	Function	Categories	Practices	Answers	References		
							CRR	C2M2	NIST
Asset management (AM)	It refers to the actions the organisation takes to identify, record and manage the organisation's critical assets.	AM1	IDENTIFY	Operation	Identify and maintain physical, software and information assets inventory with specific details.	Yes	AM.G2	ASSET.OB1f.g.h	ID.AM1
							AM.G3		ID.AM2
							AM.G4		ID.AM4
							AM.G7		PR.DS3
							AM.G6		
		AM2	IDENTIFY	Operation	Prioritise assets based on their business value, classification, and criticality.	In progress	AM.G1	ASSET.OB1c	ID.AM5
							AM.G7	ASSET.OB2c	
		AM3	IDENTIFY	Operation	Identify and archive the assets related to key critical services.	No	AM.G1	ASSET.OB1a.e	ID.AM6
							AM.G2		
		AM4	PROTECT	Control	Create information confidentiality, integrity, and availability (CIA) checking mechanism.	Not sure	CCM.G2	ARCHITECTURE.OB2	PR.DS7
							CM.G2		PR.AC5
Controls management (CM)	Control management aims to improve the security of critical services by identifying, analysing, and managing the operational environment. Controls management focuses on the control of any factors that may affect the operational environment.	AM5	PROTECT	Control	Implement measures to protect, back up, and maintain information assets and related activities (e.g., protect data-at-rest, data-in-transit; monitor data leaks).		AM.G6	ARCHITECTURE.OB2 c.e.f	PR.DS1
							CM.G2		PR.DS2
							CCM.G1		PR.DS4
									PR.DS5
									PR.IP4
		CM1	PROTECT	Operation	Define control objectives and design a control plan.		CM.G1	/	/
							CM.G3		
							AM.G5		ACCESS.OB1a.b.c.d.f.h.i
							AM.G5		PR.AC2
							CM.G2		
		CM3	PROTECT	Operation	Manage physical access to critical assets/services.		CCM.G1	ACCESS.OB3	PR.MA1
							AM.G5	ARCHITECTURE.OB3	PR.AC3
		CM4	PROTECT	Operation	Manage remote access to critical assets/services.		CM.G2	b	PR.MA2
							CCM.G1		
								ACCESS.OB2c	

Figure 14: Screenshot of CRMAM V.04 (partially).

6. Communication

This section presents the contributions of this study. The primary contribution of this study to both the knowledge base and to practice is Cyber Resilience Maturity Assessment Methodology (CRMAM), which consists of a set of constructs, a framework, and a method, according to Gregor & Hevner (2013). Following the introduction of the methodology, we also discussed the type of DSR studies it belongs to by discussing the connections between this study and theories of DSR. Secondly, this section also discusses some observations obtained during the study. It aims to highlight the problems commonly encountered by organisations in cyber resilience management and the trends in the widely used frameworks.

6.1. Contributions

As proposed by Gregor & Hevner (2013), the contributions of DSR are mainly divided into three levels: instantiations (Level 1); constructs, models, methods, design principles, and technological rules (Level 2); and design theories (Level 3). CRMAM can be seen as one of the contribution types in Level 2 (Gregor & Hevner, 2013). The methodology is made up of some of these elements: the constructs are the practices that organisations need to consider when conducting a cyber resilience maturity assessment; the framework is the groupings of practices based on different criteria, as the lens and a colour system to express the connections between practices; the methods are explanations and supplementary materials of how organisations use it to conduct an appropriate cyber resilience maturity assessment and gain a proper understanding. This methodology is designed to assist organisations in quickly conducting a maturity assessment with limited resources and time investment, considering the New Zealand environment where organisations are mostly small- or micro-sized and have insufficient capabilities. We will discuss these components in detail in the following sections.

6.1.1. Methodology

6.1.1.1. Target Audience

Azmi et al. (2018) proposed in their study that the audiences of cyber science-related frameworks can be divided into two categories: (1) audience-specific CSF and (2) across-the-board CSF.

Frameworks that focus on the first type of audience are primarily dedicated to “specific organisations that share institutional values within the originating organisation” (Azmi et al., 2018, p.267). For example, AESCSF focused on the Australian energy industry (AEMO, 2021). Another type of framework is one whose audience has general applicability. They can be used in any organisation or institution. For example, CERT-RMM is created by the government department in collaboration with academics, targeting organisations’ operational resilience management (Caralli et al., 2016). We preferred those frameworks whose audience groups are commercial organisations when selecting the reviewed frameworks because we have similar audience groups. We had no specific restrictions on the size, industry, and other attributes of organisations using this methodology.

Further, to achieve the design objective (DO4) – understandable, unambiguous, and applicable for experts and non-experts, we minimised the entry barriers and learning costs, and used a simplified way to describe concepts. It has no restrictions on the users’ role or type within organisations. Users should be able to understand and evaluate the practices of CRMAM regardless of their experience in cyber resilience. We also noticed that some micro-organisations only focus on activities that enhance business profitability due to limited capability (Williams & Manheke, 2010). They often think cyber resiliency management is activities with significant investments but no obvious benefits (Alahmari & Duncan, 2021; Fielder et al., 2016). Even some interviewees revealed that this type of organisation “stick their heads in the sand” (Interviewees I, J) and hopes they will not be targeted. Therefore, we wanted to allow those organisations to improve self-awareness by using limited resources and affordable investments.

6.1.1.2. Framework

The existing solutions in the knowledge base either contain information overload that requires significant time and resources (Carías et al., 2021) or have high entry barriers that are difficult to understand and are rarely used by organisations (Carías et al., 2019), the solution of addressing the challenge that organisations face is still desired. To achieve DO1 (comprehensive coverage and precise definition of concepts) and DO2 (essential practices and detailed descriptions), this study captured concepts from several widely used frameworks and then constituted a framework based on them. The framework contains 45 practices organisations must consider when conducting cyber resilience management and maturity assessments (Figure 15).

Based on the evaluation feedback, the 45 practices are grouped into ten domains, three categories, and five functions (Figure 15; Figure 16; Figure 17). Each grouping contains corresponding references (DO3) and categorisation, functions, domains, and colour systems to help users understand their strengths and weaknesses (DO5). This aims to provide users with options to use this methodology based on their roles, preferences, and familiarity with the widely used frameworks.

For example, Figure 15 is grouped by domains (you can find the full version of CRMAM – Version 1 here <https://osf.io/q7gpx/files/osfstorage/649bd3e1a2a2f40d324370df>). By this grouping approach, organisations can assess practices in the same domains. It helps organisations to accurately understand and identify areas that may have been missed in previous steps. However, the colour system shows that some practices are related even though they are not classified into the same domain. This relationship may be easily overlooked when focusing on one domain at a time during reviewing.

Domain	Definition	Code	Function	Categories	Practices	Answers	References		
							CRR	C2M2	NIST
Asset management (AM)	It refers to the actions the organisation takes to identify, record and manage the organisation's critical assets.	AM1	IDENTIFY	Operation	Identify and maintain physical, software and information assets inventory with specific details.	Yes	AM.G2	ASSET.OB1f.g.h	ID.AM1
							AM.G3		ID.AM2
							AM.G4		ID.AM4
							AM.G7		PR.DS3
							AM.G6		
		AM2	IDENTIFY	Operation	Prioritise assets based on their business value, classification, and criticality.	In progress	AM.G1	ASSET.OB1c	ID.AM5
							AM.G7	ASSET.OB2c	
		AM3	IDENTIFY	Operation	Identify and archive the assets related to key critical services.	No	AM.G1	ASSET.OB1a.e	ID.AM6
							AM.G2		
		AM4	PROTECT	Control	Create information confidentiality, integrity, and availability (CIA) checking mechanism.	Not sure	CCM.G2	ARCHITECTURE.OB2	PR.DS7
							CM.G2		PR.AC5
Controls management (CM)	Control management aims to improve the security of critical services by identifying, analysing, and managing the operational environment. Controls management focuses on the control of any factors that may affect the operational environment.	AM5	PROTECT	Control	Implement measures to protect, back up, and maintain information assets and related activities (e.g., protect data-at-rest, data-in-transit; monitor data leaks).		AM.G6	ARCHITECTURE.OB2 c.e.f	PR.DS1
							CM.G2		PR.DS2
							CCM.G1		PR.DS4
									PR.DS5
									PR.IP4
		CM1	PROTECT	Operation	Define control objectives and design a control plan.		CM.G1	/	/
							CM.G3		
							AM.G5		ACCESS.OB1a.b.c.d.f.h.i
							AM.G5		PR.AC2
							CM.G2		
		CM3	PROTECT	Operation	Manage physical access to critical assets/services.		CCM.G1	ACCESS.OB3	PR.MA1
							AM.G5	ARCHITECTURE.OB3	PR.AC3
		CM4	PROTECT	Operation	Manage remote access to critical assets/services.		CM.G2	b	PR.MA2
							CCM.G1		
								ACCESS.OB2c	

Figure 15: CRMAM final version – grouped by domains [Version 1] (partially).

Figure 16 shows the grouping based on categories (you can find the full version of CRMAM – Version 2 here <https://osf.io/q7gpx/files/osfstorage/649bd3e467aff80d35edfcb3>). It allows users to quickly find practices that fit their responsibilities based on their roles. The categorisation results also provide a clearer picture of the variation in maturity across three categorisations of roles and responsibilities. This makes it easier for organisations to determine weaknesses and plan for the next steps. Although this grouping reduces the layers users need to pass through to obtain the desired information, it fragments practices into three categorisations according to the performer's roles and responsibilities, which is convenient for large organisations that have capabilities to separate roles. For organisations that do not differentiate roles in this way, it might not be easy to conduct accurate and non-duplicative assessments via this grouping.

Categories	Definition	Code	Function	Domain	Practices	Answers	References		
							CRR	C2M2	NIST
Governance	The processes that identify the key business services and business activities to evaluate risk and maturity and allocate priority for guiding operations about the focus areas.	GO1	IDENTIFY	Governance	Identify and prioritise key critical services, business missions and objectives.	Yes	AM.G1	ASSET.OB1a.e	ID.AM6
		GO2	IDENTIFY	Governance	Develop a cyber resilience plan, clarify roles and responsibilities, and assign ownerships and accountabilities for cyber security.	In progress	AM.G2	ARCHITECTURE.OB1	ID.GV2
		GO3	IDENTIFY	Governance	Establish a set of relevant internal and external guidelines, policies and other obligations.	No	CM.G2	PROGRAM.OB1	ID.GV1
		VM2	IDENTIFY	Vulnerability management	Identify potential business impacts and likelihoods of each threat and vulnerability.	Not sure	CM.G2	THREAT.OB1	ID.RA4
		RM1	IDENTIFY	Risk management	Develop a strategy for identifying, analysing, and mitigating risks.		AM.G7	PROGRAM.OB2	ID.GV3
		EDM1	IDENTIFY	External dependencies management	Identify and prioritise external dependencies based on their function.		VM.G2	RISK.OB1a.b	ID.RM1
		EDM2	IDENTIFY	External dependencies management	Identify and manage the risks, threats, and vulnerabilities related to external dependencies (especially entities in the supply chain).		RM.G4	THREAT.OB1	ID.RA4
		EDM3	IDENTIFY	External dependencies management	Establish and maintain information-sharing and cooperation relationships with clients, partner organisations, and other external dependencies.		EDM.G1	THREAT.OB1a.d.f	ID.BE1
		SCM1	PROTECT	Service continuity management	Have a business continuity plan in place.		EDM.G5	THREAT.OB2c	ID.BE2
							EDG.G2		ID.BE4

Figure 16: CRMAM grouped by categories [Version 2].

Figure 17 shows the grouping based on the cyber resiliency lifecycle (you can find the full version of CRMAM-Version 3 here <https://osf.io/q7gpx/files/osfstorage/649bd3e567aff80d38edfc93>). This has similarities to the grouping approach used in NIST CSF. It provides a coherent assessment approach compared with the other two. Based on assessment results, organisations can determine their position in the cyber resiliency lifecycle. Also, for those organisations that have adopted NIST CSF or for users who are familiar with it, they can quickly familiarise themselves with it. However, this grouping requires users to jump back and forth between domains. Not only does the switching consume additional evaluation time, but it also increases the potential risks for error.

Function	Definition	Code	Domain	Categories	Practices	Answers	References			
							CRR	C2M2	NIST	CER
IDENTIFY	Develop an organisational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.	AM1	Asset management	Operation	Identify and maintain physical, software and information assets inventory with specific details.	Yes	AM.G2 AM.G3 AM.G4 AM.G7 AM.G6	ASSET.OB1f.g.h	ID.AM1 ID.AM2 ID.AM4 PR.DS3	ADM.SG TM.SG1 KM.SG KM.SG KM.SG
		GO1	Governance	Governance	Identify and prioritise key critical services, business missions and objectives.	In progress	AM.G1 AM.G2	ASSET.OB1a.e	ID.AM6	ADM.SG
		EDM1	External dependencies management	Governance	Identify and prioritise external dependencies based on their function.	No	EDM.G1 EDM.G5	THRD- PARTIES.OB1a.d.f	ID.BE1 ID.BE2 ID.BE4	EXD.SG EXD.SG EXD.SG
		AM2	Asset management	Operation	Prioritise assets based on their business value, classification, and criticality.	Not sure	AM.G1 AM.G7	ASSET.OB1c ASSET.OB2c	ID.AM5	SC.SG2 KM.SG
		AM3	Asset management	Operation	Identify and archive the assets related to key critical services.		AM.G1 AM.G2	ASSET.OB1a.e	ID.AM6	ADM.SG ADM.SG
		EDM3	External dependencies management	Governance	Establish and maintain information-sharing and cooperation relationships with clients, partner organisations, and other external dependencies.		EDM.G3	/	PRAT3	EXD.SG EXD.SG
		EDM3	External dependencies management	Governance	Establish and maintain information-sharing and cooperation relationships with clients, partner organisations, and other external dependencies.		EDM.G3	/	PRAT3	EXD.SG EXD.SG
		GO2	Governance	Governance	Develop a cyber resilience plan, clarify roles and responsibilities, and assign ownerships and accountabilities for cyber security.		CM.G2	ARCHITECTURE.OB1 PROGRAM.OB1 PROGRAM.OB2	ID.GV2	RBD.SG RBD.SG COMP.SG COMP.SG COMP.SG COMP.SG COMP.SG CTRL.SG IC.SG RTM.SG MON.SG OTA.SG OTA.SG OTA.SG
		GO3	Governance	Governance	Establish a set of relevant internal and external guidelines, policies and other obligations.		CM.G2 AM.G7	PROGRAM.OB1 PROGRAM.OB2	ID.GV1 ID.GV3	COMP.SG CTRL.SG IC.SG RTM.SG MON.SG OTA.SG OTA.SG OTA.SG
		TA2	Training and awareness	Operation	Design training lessons to meet the cyber resilience objectives.		TAG1	WORKFORCE.OB2	/	OTA.SG OTA.SG OTA.SG

Figure 17: CRMAM grouped by lifecycle [Version 3].

It is worth noting that we used a colour system in each version to emphasise the relations between practices. The practices with the same colour can be assessed together, and the different darkness implies a correlation between them and the order in which they are assessed. Although some practices are not grouped into the same domain or function, they are still relevant and can be reviewed together, as AM1, GO1, and EDM1 in Figure 17. The purpose of this is to convey the relevance of the practices clearly to the user and to aid with the order of assessment.

6.1.1.3. Supplementary Materials

We also developed some supplementary materials to help users better understand the methodology. We defined the definition of governance, operations, and controls through a literature review and created a relationship map (Figure 18) to explain their relationships.

- Governance:** The processes that identify the key business services and business activities to evaluate risk and maturity and allocate priority for guiding operations about the focus areas.
- Operations:** The combination of people, processes, and controls to manage and mitigate the risk of business services and maintain business activities.
- Controls:** A set of tools, methods, procedures, and actions that should be taken by organisations to protect business services and business activities.

We view this diagram as the environment in which the organisation conducts its business activities. The organisation uses and allocates assets (people, process, technology) through governance, operations, and controls. Governance provides guidance and directions to operations and controls (Harris & Martin, 2021; Jensen, 2019). Operations and controls install specific strategies to processes. Governance is also influenced by operations and controls to improve decisions (Carías et al., 2021; Huang et al., 2022). This interactive influence also exists between operations and controls. The “Governance – Operations – Controls” needs to be a continuous improvement cycle. Although controls are the most fundamental level, their influence is not suppressed. In some SMEs, the countervailing influence of controls often occupies the more prominent part of these three categories, according to interviewees’ responses.

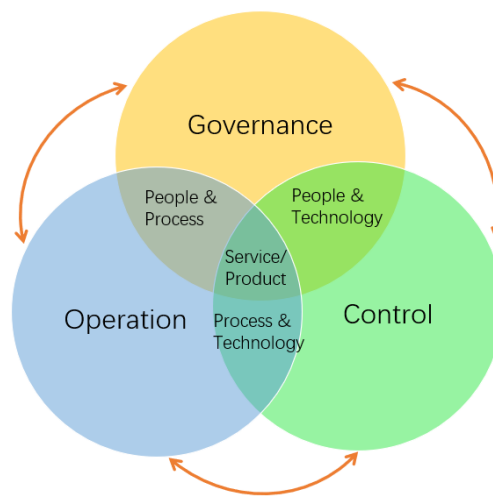


Figure 18: Relationship map.

In CRMAM, we argue that organisations should consider four aspects when evaluating practices: people, process, technology, and information. There are two reasons for doing so. Firstly, based on the literature review and interviews with organisational representatives, it is clear that organisations typically involve these four assets in conducting business activities: people, information, technology, and facilities (CISA, 2016a). As mentioned before, we grouped technology and facilities together as they can broadly refer to the infrastructures used in organisations. Some aspects, like processes, are often overlooked in cyber resilience reviewing because of their invisibility. Some academics are gradually emphasising the importance of the correctness and effectiveness of “process” in cyber resilience (Carayannis et al., 2021; Carías, Arrizabalaga et al., 2020; Yusif & Hafeez-Baig, 2021). Carayannis et al. (2021) pointed out the importance of creating dynamic processes to identify intangible organisational assets, resources, and capabilities to enhance cyber resilience. Similarly,

Onwubiko (2020) noted that having the right processes in place for resilience and recovery from cyber incidents is a challenging but essential task. Therefore, organisations should carefully consider the process's integrity and correctness.

To assist organisations in accurately assessing their practices from these four aspects, we devised a reference sheet (Figure 19). This reference sheet is considered as supplementary material (rather than being present in the framework) because we want to minimise the complexity of the methodology. Those users with sufficient experience and familiarity with how to utilise assessment can focus on the practice reviewing without the distraction of the reference sheet. For those users who do not have this expertise, we provide them with an option to use the reference sheet to enrich their understanding and guide each aspect of the practice (you can find the full version of CRMAM – reference sheet here <https://osf.io/q7gpx/files/osfstorage/649bd3e23809110c913c33ca>).

Code	Practices	Sub-categories	
		Name	Question
AM1	Identify and maintain physical, software and information assets inventory with specific details	People	Are people assets (human resources) inventory identified and maintained periodically with specific details?
		Process	Are process related assets inventory identified and maintained periodically with specific details?
		Technology	Are technology assets inventory identified and maintained periodically with specific details (technology includes hardware, software, and external information systems)?
		Information	Are information assets inventory identified and maintained periodically with specific details?
AM2	Prioritise asset based on its business value, classification, criticality	People	Are people related assets prioritised based on their business value, classification, and criticality?
		Process	Are process related assets prioritised based on their business value, classification, and criticality?
		Technology	Are technology related assets prioritised based on their business value, classification, and criticality?
		Information	Are information related assets prioritised based on their business value, classification, and criticality?
AM3	Identify and archive the assets related to key critical services	People	Are people assets related to key critical services identified and recorded?
		Process	Are process assets related to key critical services identified and recorded?
		Technology	Are technology assets related to key critical services identified and recorded?
		Information	Are information assets related to key critical services identified and recorded?
AM4	Create information confidentiality, integrity, availability (CIA) checking mechanism	People	Are CIA requirements used to determine which people are authorised to maintain information assets?
		Process	Has a process for creating and managing the CIA checking mechanism been implemented?
		Technology	Are technologies in use to support the CIA checking mechanism?
		Information	Is the CIA checking mechanism performed for information assets?

Figure 19: Reference sheet for sub-categories.

6.1.1.4. Connections with DSR Studies

livari (2015) proposed two research strategies for DSR. Strategy 1 is to find the problem from the literature and then create an artefact to solve this problem through DSR. This process does not necessarily involve real-world clients when identifying problems. Researchers evaluate its reliability via evaluation after designing. Strategy 2 starts with researchers communicating with clients to identify real-world problems in practice and then using DSR to conduct targeted research and propose solutions to problems. The researchers generalise artefacts as a contribution to the

knowledge base during the research process. We communicated with practitioners in the cyber resilience area to identify a problem they encountered in practice. We analysed the knowledge base to determine the necessity of a solution, making this study a Strategy 2 study. Then, we conducted four Design Cycles under the guidance of the DSR process model (Peffer et al., 2007) to create CRMAM.

Furthermore, Venable et al. (2016) suggested that the evaluation of DSR artefacts can provide evidence of whether the theory of design can solve problems or make improvements. They proposed two types of evaluation: naturalistic (e.g., the case study of a real-world environment) and/or artificial (e.g., literature analysis, lab experiments) to determine whether artefacts are well-designed. We used artificial evaluation by interviewing experts (Nagle et al., 2020; Venable et al., 2016) to determine the “utility, quality, and efficacy” of the artefact” (Hevner et al., 2004, p.85). In our study, representatives from different industries were invited to perform each evaluation but the study is artificial in nature as they did not implement the artefact in their environments in this instance.

In addition, Nunamaker et al. (2015) divided the practices of DSR into three categories: proof-of-concept (researchers design a feasible solution to the problem and present the functionality of the solution), proof-of-value (researchers determine whether the created solution is more efficient than original solutions via stakeholder’s testing), and proof-of-use (researchers define whether practitioners can successfully obtain value from the solution and solve the problem). In the current research, we designed CRMAM with the concepts identified from the knowledge base towards solving the problem from the practice. Its functionalities are evaluated through three rounds of evaluations, and explained in detail in the previous sections, which can be viewed as a proof-of-concept.

6.1.2. Methodology as Contribution

6.1.2.1. To Practice

The review of the practice and knowledge base revealed that organisations’ cyber resilience practices are primarily one-sided, with a narrow focus on information security protection or the adoption of emerging security technologies, resulting in unnecessary resources spent to achieve

resilience (Arora et al., 2004; Fielder et al., 2016). Academics thus argued that organisations are underprepared for cyber resilience because they either underestimate cyber risks or misestimate their preparedness (Alahmari & Duncan, 2021; Spremić & Šimunic, 2018). One of the root causes for the emergence of this phenomenon is their lack of cyber resilience understanding and maturity review.

Despite attempts by practitioners and academics to help them build this understanding by providing a plethora of frameworks and recommendations about practices, these solutions are not fully utilised by organisations. We believe that there are a variety of reasons for this. One of the most prominent is that the existing cyber resilience frameworks contain an overload of detail and information, which requires organisations to have sufficient resources to understand and adopt the frameworks (Carías et al., 2021). Some organisations, especially SMEs, have limited resources to allocate to their cyber resilience management. Thus, they are not able to use these frameworks properly with their affordable capabilities (Carías, Arrizabalaga, et al., 2020). Moreover, large organisations with enough resources to support the adoption of these frameworks have more people, processes, and assets that need to be considered while reviewing. A lengthy framework often means longer review time and broader review scope. While the level of detail and coverage of these frameworks work positively in guiding practices, most organisations prefer that cyber resiliency reviews are achieved efficiently and effectively, according to interviewees from large organisations. Based on these needs, we provide practitioners with a methodology to properly conduct assessments with a low use barrier and fewer resource requirements.

In contrast to the professional frameworks, we recognise that CRMAM does not contain that level of detailed explanations and suggestions around specific practices. However, CRMAM has no less coverage than those frameworks regarding the domains and concepts that need to be considered. It contains ten domains and 45 practices of cyber resilience management and highlights four aspects to consider when assessing these practices. On top of this, CRMAM analyses and interprets cyber resilience management from a high-level perspective, providing a solution for organisations that are seeking a foundational understanding of their cyber resilience maturity. Compared to professional frameworks that require organisations to spend a few weeks or even months understanding and implementing dozens or hundreds of pages of details, our methodology takes less time and resources for organisations to conduct a proper self-assessment. Based on the results of the

assessment, organisations can have a clear understanding of their maturity level and make decisions about whether to engage in in-depth cyber resilience practices to improve maturity. Our methodology lowers the entry barriers, allowing SMEs with limited resources to adopt while ensuring the functionalities to meet the needs of large organisations.

6.1.2.2. To the Knowledge Base

In identifying the problems raised by practitioners, we found that researchers rarely examine the state of cyber resilience maturity around New Zealand. Most studies that address this context (e.g., Christine & Thinyane, 2020a, 2020b) discussed it as part of an overall cyber resilience analysis for larger regions (e.g., Asia-Pacific in Christine & Thinyane's study (2020a)). Most of the frameworks commonly used by researchers (e.g., NIST CSF, CRR) are developed around the U.S., U.K., and other larger countries. Their environment and context differ significantly from New Zealand. Although some frameworks offered modified versions for small organisations, they are still challenging to use in a reasonable way. Thus, there is a lack of suitable tools for researchers to analyse cyber resilience maturity in New Zealand. This shortage also affects related research activities in studying cyber resilience in countries with similar attributes to New Zealand, which have many small- and micro-organisations.

This study provides researchers with a methodology as the tool that can assist them in understanding cyber resilience and cyber resilience maturity. To make this tool applicable to all types of organisations (e.g., organisations focused solely on the domestic market and multinational firms that operate worldwide), it is designed with consideration about generalisation. Therefore, this methodology contains no concepts specific to a single industry or context. The researcher can install it without type restriction of organisations. Meanwhile, it reduces learning costs and entry barriers, users can understand the concepts and practices properly regardless of whether they have sufficient experience in cyber resilience management. This reduces the workload required by the researcher in terms of interpretation and communication when using it as a data collection tool with the organisation's users.

In addition, the comparison of frameworks conducted during the study can also be seen as a contribution to the knowledge base. We created a weighting matrix and used it to make a detailed comparison of the captured frameworks. This matrix contains a detailed scoring system and

applicable assessment criteria. Although some similar evaluation matrixes have been mentioned in other studies (Benz & Chatterjee, 2020; Carías et al., 2021), the matrix we created not only contains the criteria that academics would refer to when making comparisons (as in most studies) but also adds some practical criteria based on advice provided by practitioners, which are not presented in other studies. This makes the matrix more relevant to practitioners' actual solution-seeking process in the real-world environment. Meanwhile, our study provided a detailed evaluation of the widely used frameworks. All practices mentioned were compared and discussed in terms of coverage and details. This framework comparison will be helpful to other researchers studying cyber resilience frameworks.

6.2. Observations

In the Design Cycles, we obtained some interesting findings by reviewing the knowledge base and interviewing different types of respondents.

6.2.1. Trends of Concepts in Cyber Resilience Management

Firstly, one of our findings when analysing and capturing concepts related to cyber resilience is that most frameworks, approaches, and theories related to cyber resilience are generally around a few popular areas (Benz & Chatterjee, 2020; Caralli et al., 2016; CISA, 2020b) such as asset management, risk management, and incident management. This general focus of attention is an excellent emphasis to some extent, yet we argue that it can also create a misconception among organisations: they may have a narrow view that cyber resilience management only revolves around these areas, then neglect to manage them at a macro and holistic level. This opinion was evident in our interviews with interviewees from commercial organisations.

Secondly, we found that some “novel” concepts are becoming popular, such as workforce management (Muneer, 2022), cyber security architecture (Muneer, 2022), and environmental management (Caralli et al., 2016). One of the possible reasons for this new trend is that there is a growing awareness that rapid technological advances are leading to a mismatch between technology and humans, as employees do not have enough time to familiarise themselves with outpacing technology (Curtis et al., 2009; Iovan & Iovan, 2016; van der Kleij & Leukfeldt, 2020). The most direct consequence of this gap is the proliferation of cyber incidents caused by human errors (Huang &

Pearlson, 2019). Therefore, organisations are suggested to train employees according to the employment lifecycle to narrow the gap between technology and employee (Caralli et al., 2016). Another possible reason is the growing awareness that cyber resilience is an evolving process and that cyber resilience management is a forward-planning action (Muneer, 2022). The dated practice of passively upgrading cyber resilience in response to cyber events that have already occurred no longer deters attackers. Organisations must proactively plan ahead by considering their resources, capabilities, needs, and other relevant factors. As a result, designing a cyber security architecture is becoming increasingly popular.

6.2.2. Lack of Practices Related to Governance in three Functions.

We argue that organisations' activities are mainly associated with three categorisations (governance, operations, and controls) based on their workloads and responsibilities. Organisations should also start with these three categories when considering cyber resiliency management practices. The lifecycle (Identify, Protect, Detect, Respond, and Recover) represents a coherent way of cyber resilience management (Azmi et al., 2018). We attempted to assess the practice coverage of CRMAM by these two criteria. After completing all the Design Cycles, we presented the practices by category and function in Figure 20.

		Categorisation		
		Governance	Operation	Control
Function	Identify	GO1, GO2, GO3 VM2, RM1, EDM1, EDM2, EDM3	AM1, AM2, AM3, VM1, TA2,	-
	Protect	SCM1, EDM4, TA1	CM1, CM2, CM3, CM4, CM5, CC3, CC4, SCM2, EDM6, TA3, TA4, TA5	AM4, AM5, CC1, CC2
	Detect	-	VM4, IM1, IM2, EDM5	-
	Response	-	VM3, IM3, SCM3, RM2, RM3, RM4	-
	Recover	-	GO4, IM5	IM4

Figure 20: Comparison of practices by categories and functions.

From this figure, we found that governance-related practices only appear in the identify and protect phases. We conducted another framework review and found that these frameworks discussed little advice on governance in these three phases (Detect, Respond, And Recover) (Caralli et al., 2016; CISA, 2020b; Muneer, 2022; NIST, 2018). In contrast, they focused much more on operations and

controls than expected. The potential impact of this neglect of governance by these frameworks is significant. The most apparent manifestation is the inability of organisations using these frameworks to acknowledge the role of governance actively. This results in organisations potentially missing governance roles in managing all aspects of operational environments, including cyber resilience.

Although some academics may be aware of the absence of governance in practice in their studies (Bodeau et al., 2010; De Bruin & Von Solms, 2016; Savaş & Karataş, 2022), frameworks, like NIS CSF 2.0, are also starting to enhance their focus on governance in the upcoming versions, this message has not been effectively transmitted to organisations. Therefore, the absence of governance in cyber resilience management may still result in organisations missing out on critical decision-making processes, effective risk management and overall strategic planning related to cyber resilience. Other than that, we note that CRMAM does not include many practices on controls. Our explanation for this is that we wanted to provide a methodology to assist organisations in gaining an understanding from a high-level rather than tell them how to conduct cyber resilience practices through specific controls.

6.2.3. Concerns of Governance in Organisations

As mentioned above, one fallout with these frameworks providing less governance-related advice is that organisations neglect governance as a functional category. This is corroborated by the interviewees' concerns about the absence of governance in cyber resilience management. Some interviewees with experience in helping organisations manage cyber resilience declared that one of the root causes of most cyber resilience failures is a failure at governance. This manifests itself in three specific ways. Firstly, there is a lack of awareness of cyber resilience management in governance (Andronache, 2021; Georgiadou et al., 2022). During our interviews, we found that governance in some organisations only realised the need for cyber resilience management after experiencing a serious cyber incident and suffering significant losses. Before that, they usually had a low interest in and awareness of governance. Damages to reputation and clients' trust might be irreversible, even if the situation is repaired.

Secondly, there is a lack of involvement in cyber resilience management at governance (Musa, 2018; Zwikael, 2008). Some organisations are aware of this, but the performers in governance are rarely involved in the actual development and guidance of resilience management (Jensen, 2019; Musa,

2018). They might often wander between “we should have a solution” and “we already have a solution” but do not participate in developing management action. Not only do they not guide organisations’ cyber resilience goals and direction, but they also do not understand operations and controls and configurations needed to execute effectively.

Thirdly, there is a lack of support for cyber resilience management at governance (Gutierrez et al., 2015; Iovan & Iovan, 2016; Zwikael, 2008). Interviewees with experience in helping organisations manage cyber resilience revealed that some organisations who want to improve cyber resilience often stop at the preliminary assessment stage or temporarily pause cyber resilience improvement due to several reasons, such as funding issues, changing development goals, and questioning from the top management (Onwubiko, 2015; Wong et al., 2022). If managers of governance fail to recognise the importance of reflecting on identified cyber resilience issues, they, as decision-makers, may lose confidence and support for maturity assessment and improvement, ultimately leading to failure in cyber resilience management (Garcia-Perez et al., 2021). While these interviewees emphasised that the choice to “ignore” identified cyber resilience issues may not always be entirely negligent, some organisations still experienced serious consequences for such decisions.

We therefore argue that the root cause of this situation is a lack of understanding and ownership of cyber resilience management at an organisation’s governance. Because organisations fail to properly understand the need for and benefits of cyber resilience management and only overemphasise the inputs and expenditures in the management process (operations and controls), this leads them to misalignment and underestimation of the hazards of cyber incidents and the role of becoming a resilient organisation to withstand them.

6.2.4. Lack of Understanding of the Organisation's Maturity

During the evaluation process, we asked interviewees who were the employees responsible for their entity’s organisational cyber security about their understanding of its cyber resilience maturity. Some organisations considered themselves at least “roughly” at a middle level based on their current cyber security practices. However, such statements are fraught with uncertainty and ambiguity. This is because these conclusions might not be made based on accurate assessment results by standards or frameworks. They are more like a judgment made from personal subjective feelings. Other organisations acknowledged their lack of knowledge related to cyber resilience

maturity and therefore did not have a clear understanding of where they are and lacked a clear vision of their future development goals. Furthermore, these organisations often assumed that more cyber resilience practices (operations and controls) mean a higher maturity level of resilience. Based on this situation, we believe that organisations' understanding of the "maturity" of cyber resilience is still at a relatively basic level.

7. Limitations

Firstly, we added ISO 27001 as the reviewed framework in the second Design Cycle to respond to the evaluator's suggestions. However, since all resources about ISO 27001 are behind a paywall, we can only use the crosswalk document provided by CRR (Homeland Security, 2014) as the reference for ISO 27001. The issue raised in this way is that the accuracy is not highly guaranteed as we cannot compare the original descriptions in ISO 27001. For instance, the description AM1 in CRMAM responds to ID.AM1 and ID.AM2 in NIST CSF. According to the crosswalk (Homeland Security, 2014), these two items respond to ISO/IEC 27001: 2013 A.9.1.1, A.9.1.2, A.9.1.3. We are not able to ensure that the description of AM1 in CRMAM responds accurately to these suggestions mentioned in ISO 27001 without seeing the actual descriptions. Although we believe that the crosswalk provided by CRR has reliable accuracy, the lack of comparison to the actual text in ISO 27001 is one of the limitations needed to be mentioned.

Secondly, we reviewed and captured the concepts from the reviewed frameworks: CRR, NIST CSF, C2M2, CERT-RMM, and ISO27001. These widely used frameworks have been applied in diverse types and sizes of organisations worldwide, including New Zealand organisations. However, some reviewed frameworks, such as NIST CSF, CERT-RMM, are designed based on US government departments. They do not include customised concepts for the New Zealand environment. Although we designed CRMAM with the consideration for New Zealand's SMEs and micro-organisations in mind, CRMAM does not include any New Zealand-focused practices. One consideration regarding this limitation is that we noticed during interviews that some small organisations, although very small compared to some large multinational organisations, are not limited to the New Zealand domestic market, but are conducting business with global clients. Therefore, a methodology that is not over-tailored to meet a particular country's environment might be more suitable for their needs.

In addition, it needs to be admitted that our interpretation of maturity is still limited. The final version of CRMAM contains two representations of the maturity results: a point system and a graphical representation. Both representations help users to understand the results and provide a picture of their maturity position. They still have certain drawbacks. We treated all practices equally so that each selection received the same score (e.g., each 'Yes' counts as 2 points). However, the framework review and interviews revealed that organisations might place different importance on domains according to business activities. Further, practices in the same domain might also gain different levels of attention. The interviewees' concerns about governance also imply that more attention should be paid to governance-related practices. Therefore, the same score does not reflect this difference. Moreover, both representations were added in the last Design Cycle. Unfortunately, we did not have the opportunity to conduct another evaluation of them.

8. Future Work

To achieve the goal of helping practitioners solve their problems in cyber resilience management, we designed CRMAM through four Design Cycles. With a more detailed understanding of this area, along with study and more feedback received, we have some ideas about how to improve CRMAM in the future. The future work should contain two aspects.

Firstly, it is necessary to conduct the proof-of-use or proof-of-value study of CRMAM. We agree with some researchers who have emphasised the importance of proof-of-use (Nagle et al., 2020; Nunamaker et al., 2015) and believe that CRMAM should be tested for proof-of-value and proof-of-use to assess its actual usefulness as a solution and to help further improve its design. Unfortunately, we did not conduct real-world testing as it is out-of-scope. In future studies, proof-of-value and proof-of-use related research about CRMAM should be conducted. To achieve this, we need to test the methodology in real-world environments and obtain further results, such as whether it makes the organisation's assessment process more accurate and effective than the existing solution. What metrics should be used to evaluate CRMAM's value and how does it meet or exceed them? What benefits do practitioners derive from using CRMAM? Does CRMAM fit into the existing assessment processes of the practitioners? What challenges or difficulties do practitioners encounter when using it?

Secondly, we need to identify and add governance-related practices in detect, respond, and recover

phases. By comparing the practices using categories and functions, we found that the practices in CRMAM do not cover all phases, especially the absence of governance-related practices in detect, response, and recover phases. Although we believe this is due to the neglect of related suggestions in the reviewed frameworks, we still acknowledge that this absence needs to be fixed. In future work, a more extensive review is needed to determine the importance of governance in these phases and the practices that need to be performed.

Thirdly, we need to define the importance of the three categorisations. During the interviews, we noticed that the structure of organisations regarding cyber resilience might be influenced by organisational attributes (e.g., size, type, industry). This was evident in the literature (Chen et al., 2011; Samonas et al., 2020; Tsen et al., 2022). However, due to the limited data, we could not clearly distinguish specific trends between such differences and influencing factors. In future studies, this trend may be confirmed by larger data collection. Also, some interviewees mentioned that organisational attributes might influence the importance of three categorisations to organisations. Consultancy organisations may rely more on governance and operations, while organisations in manufacturing care more about controls. Although most interviewees claimed that their organisations treat all three equally, we would like to test this statement in future studies.

Similarly, before evaluating the three versions of groupings, we proposed a scenario aiming to discover the interviewees' preferences for different versions, then based on this preference, provide users with the version that suits them when presenting the methodology. For example, provide suggestions of versions according to users' usage habits or the stage of cyber resiliency management that the organisation is in. We discussed these scenarios with the research team and expected to add this as a part of the explanations in supplementary materials. Unfortunately, despite noticing this trend slightly based on the data we obtained, we did not gather enough evidence to make suggestions from this perspective. This thinking could be a direction for future work and achieved by larger data collection.

Fourthly, make some practical modifications. Some suggestions received from the third evaluation should be adopted. Firstly, provide a toolkit containing usage examples and create roadmaps based on the review results. To reduce complexity, CRMAM contains only the necessary text-based information. It is undeniable that examples of instantiation would help to understand better.

Providing supporting documentation on CRMAM instantiation may be needed. Secondly, we realised the limitations of using an Excel-based tool. Most similar tools on the marketplace are software-based, and such a format can significantly enhance the flexibility of the CRMAM. Also, if sufficient evidence of user preferences for different versions can be obtained in future studies, a software-based tool can create a pre-step to obtain information and populate the appropriate version.

Later in this study, we realised that organisations might expect help in future directions after defining maturity, such as developing target maturity levels and comparing current maturity with target maturity to determine improvements and roadmap. Therefore, more explanation and support regarding maturity are required. One solution is adding evaluation tables of current and future state assessments to CRMAM. Organisations can determine the future state while reviewing each practice and finally obtain a maturity result on the current state and a development plan for the future state.

9. Conclusion

With the increasing severity of cyberattacks, organisations must endure the threat of cyberattacks when conducting business activities. Reactive remediation of losses from cyber incidents is not the fundamental solution to this dilemma, organisations should proactively understand their cyber resilience maturity and work toward a higher level of resilience maturity (Benz & Chatterjee, 2020; DeMarco, 2018; Karjalainen & Kokkonen, 2020). A comprehensive understanding of cyber resilience and maturity is an essential prior step (Yusif & Hafeez-Baig, 2021). To help them gain this understanding, this study designs a methodology (CRMAM) guided by a DSR process model (Peppers et al., 2007). It is created based on frameworks related to cyber resilience captured from the knowledge base. CRMAM went through four Design Cycles. Each cycle consists of three phases of design – build – evaluate, and academics and practitioners were invited to conduct the evaluations.

For organisations that do not have sufficient resources and financial support, understanding where they are in terms of cyber resilience maturity can be a difficult challenge. This methodology helps organisations use their limited resources to self-assess their existing cyber resilience practices and understand their maturity. It incorporates all the necessary aspects of cyber resilience management that organisations need to consider. Based on evaluations of Design Cycles, it was generally agreed by evaluators to allow organisations to take a quick assessment and determine where they stand

from a high-level perspective. Based on the assessment results, organisations can decide whether to undertake deeper cyber resilience management and significant investment. Meanwhile, the methodology can be used as a research tool to assist with research around the maturity of cyber resilience in countries like New Zealand with many SMEs or micro-organisations.

It is worth mentioning that CRMAM has also been made freely available on Open Science Framework (A online research platform for researchers to plan, analyse and share their work transparently)(Foster & Deardorff, 2017). Organisations and academics can acquire resources and provide feedback for CRMAM. This not only increases the likelihood of being used to some extent, but also reduces the obstacles that the final research mile (Nagle et al., 2020; Nunamaker et al., 2015) cannot be completed because of the issues that practitioners encounter in obtaining academic results.

Appendices

Appendix A

The interview questions used in Design Cycle 2.

Interview question list

Part 1 - Introduction

1. What is your name and position? How long have you been working in this area?
2. What kind of service does your agency provide?
3. Could you please describe your role in the cyber security area? What does the profession entail?
4. Could you please describe what cyber resilience means to you and your agency?
5. Do you see Cyber Resiliency as different from Cyber Security? Why?
6. Are you actively utilising any frameworks for your Cyber Resiliency journey? YES / NO
 - **YES:** What frameworks/tools did you use? Which one do you recommend?
 - **NO:** Do you know any frameworks/tools that organisations use?
7. Will you follow the instructions/procedures recommended in these frameworks when using them?

Part 2 – Review of Artefact

1. Do you understand the practices of each domain? Do they make sense to you, or would you suggest any changes?
2. Do the definitions of Governance, Operations and Controls make sense to you?
3. Could you please appreciate the need to link from 3 categories and the need to have all three to enable effective Cyber Resiliency?
4. Will you evaluate these three categories as equally important?
5. Would you consider yourself operating in a Governance, Operations or Controls space around Cyber security?
6. Could you please look at the categorisations of each practice – from your understanding, are they reasonable?
7. Do you think the categorisations help you prioritise the practices or identify the weaknesses in the current cyber resilience plan?
8. What do you think needs to be improved?

Part 3 – Cyber Resilience Maturity

1. What is your understanding of cyber resilience maturity?
2. Do you have any procedure(s), or frameworks, for defining and analysing it?
3. What criteria do you think is a must-have for evaluating cyber resilience maturity?
4. How do you manage and measure continuous improvement for Cyber Resiliency?

Appendix B

The interview questions used in Design Cycle 3.

Interview question list

Part 1 - Introduction

1. What is your name and position?
2. What is your organisation's size? What kind of service does your organisation provide?
3. What is the structure of your organisation regarding cyber security?
4. Could you please describe your role in the cyber security area? How long have you been working in this area? What does the profession entail?
5. Could you please describe what cyber resilience means to you and your organisation?
6. Do you see Cyber Resiliency as different from Cyber Security? Why?
7. Are you actively utilising any frameworks for your Cyber Resiliency journey? YES / NO
 - **YES:** What frameworks/tools did you use? Which one do you recommend?
 - **NO:** Do you know any frameworks/tools that organisations use?
8. Will you follow the instructions/procedures recommended in these frameworks when using them?
9. Has your organisation been attacked/ experienced cyber incidents in recent years? How does your organisation respond or recover?
10. Will you follow the cyber security plan you have created when mitigating risk or responding to incidents?

Part 2 – Review of Artefact

1. Do you understand the practices of each domain? Do they make sense to you, or would you suggest any changes?
2. Do the definitions of Governance, Operations and Controls make sense to you?
3. Would you consider yourself operating in a Governance, Operations or Controls space around Cyber security?
4. Will you evaluate these three categories as equally important?
5. Could you please appreciate the need to link from 3 categories and the need to have all three to enable effective Cyber Resiliency?
6. Could you please look at the categorisations of each practice – from your understanding, are

they reasonable?

7. Do you think the categorisations help you prioritise the practices or identify the strengths and weaknesses in the current cyber resilience plan?
8. Are the sub-categories of each practice understandable for you? Do you think the reference sheet is needed to help you understand?
9. Which version do you prefer to use?
10. What do you think needs to be improved?

Part 3 – Cyber Resilience Maturity

1. What is your understanding of cyber resilience maturity?
2. Do you know your organisation's maturity level? Does your organisation understand its maturity level?
3. Do you have any procedure(s) or frameworks for defining and analysing it?
4. What criteria do you think are the must-have for evaluating cyber resilience maturity?
5. How do you manage and measure continuous improvement for Cyber Resiliency?

Appendix C

Table 15: Interviewee's attributes.

No.	Title	Working experience (years)	Categorisation	Organisation size	Services
A	CISO	5 – 10	Governance, operations	Large	IT services, platform development, business advisories
B	Director	5 – 10	Governance, operations	Micro	Cyber resilience services and consultancy
C	Cloud platforms and engineering practice lead	10 – 15	Governance, operations, controls	Large	IT cloud service, application development
D	Architecture security manager	0 - 5	Operations, controls	Large	Education service
E	CISO	10 -15	Governance	Large	Direction for public service
F	COO	10 -15	Governance, operations, controls	Medium	Cyber security training and education
G	CIO	20 – 25	Governance, operations	Large	Healthcare service
H	Senior security architecture	10 – 15	Governance, operations, and controls	Large	Cloud-based accounting software

I	Director; CISO	15 – 20	Governance	Micro	Information security professional services consulting
J	Lead information technology security manager	5 – 10	Governance, operations	Large	Managed service provider, application development service

References

- AEMO. (2021). *Australian Energy Sector Cyber Security Framework (AESCSF) Framework Overview*.
<https://www.energy.gov.au/government-priorities/energy-security/australian-energy-sector-cyber-security-framework>
- Alahmari, A. A., & Duncan, R. A. (2021). Investigating Potential Barriers to Cybersecurity Risk Management Investment in SMEs. *Proceedings of the 13th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2021*, 0–5.
<https://doi.org/10.1109/ECAI52376.2021.9515166>
- Alqahtani, M., & Braun, R. (2021). *Examining the Impact of Technical Controls , Accountability and Monitoring towards Cyber Security Compliance in E-government Organizations*. 1–40.
<https://doi.org/10.21203/rs.3.rs-196216/v1>
- Andronache, A. (2021). Increasing Security Awareness Through Lenses of Cybersecurity Culture. *Journal of Information Systems & Operations Management*, 15(1), 7–22.
<https://www.proquest.com/scholarly-journals/increasing-security-awareness-through-lenses/docview/2571982600/se-2?accountid=14542>
- Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient systems. *COMPUTERS & INDUSTRIAL ENGINEERING*, 149(January), 106829.
<https://doi.org/10.1016/j.cie.2020.106829>
- Annarelli, A., & Palombi, G. (2021). Digitalization Capabilities for Sustainable Cyber Resilience: A Conceptual Framework. *SUSTAINABILITY*, 13(23). <https://doi.org/10.3390/su132313065>
- Arora, A., Hall, D., Pinto, C. A., Ramsey, D., & Telang, R. (2004). Measuring the Risk-Based Value of IT Security Solutions. *IT Professional*, 6(December), 35–42.
<https://doi.org/10.1109/MITP.2004.89>
- Aura News. (2021). *Aura Cyber Security Market Research 2021 - Kiwi businesses report being targeted by cyber-attacks*. Kordia. <https://www.kordia.co.nz/news-and-views/cyber-research-21>
- Azmi, R., Tibben, W., & Win, K. T. (2018). Review of cybersecurity frameworks: context and shared concepts. *Journal of Cyber Policy*, 3(2), 258–283.
<https://doi.org/10.1080/23738871.2018.1520271>
- Bellini, E., & Marrone, S. (2020). Towards a novel conceptualization of Cyber Resilience. *Proceedings of 2020 IEEE World Congress on Services, SERVICES 2020*, 189–196.

<https://doi.org/10.1109/SERVICES48979.2020.00048>

Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures.

Proceedings of 7th International Conference on Financial Criminology 2015, 28(April), 24–31.

[https://doi.org/10.1016/s2212-5671\(15\)01077-1](https://doi.org/10.1016/s2212-5671(15)01077-1)

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs.

BUSINESS HORIZONS, 63(4), 531–540. <https://doi.org/10.1016/j.bushor.2020.03.010>

Birkle, C., Pendlebury, D. A., Schnell, J., & Adams, J. (2020). Web of science as a data source for research on scientific and scholarly activity. *Quantitative Science Studies*, 1(1), 363–376.

https://doi.org/10.1162/qss_a_00018

Bissell, K., Fox, J., Lasalle, R., & Cin, P. D. (2021). *The State of Cybersecurity Report 2021 _ 4th Annual Report _ Accenture*. Accenture. [https://www.accenture.com/nz-](https://www.accenture.com/nz-en/insights/security/invest-cyber-resilience)

[en/insights/security/invest-cyber-resilience](https://www.accenture.com/nz-en/insights/security/invest-cyber-resilience)

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber Resilience – Fundamentals for a Definition. In A. Rocha, A. Correia, S. Costanzo, & L. Reis (Eds.), *New Contributions in Information Systems and Technologies* (Vol. 353, pp. 311–316). Springer International Publishing. <https://doi.org/10.1007/978-3-319-16486-1>

Bodeau, D., Boyle, S., & Fabius-green, J. (2010). Cyber Security Governance A Component of MITRE 's Cyber Prep Methodology. In *MITRE technical report* (Issue September).

<https://www.mitre.org/publications/technical-papers/cyber-security-governance>

Bodeau, D., Graubart, R., Picciotto, J., & McQuaid, R. (2012). Cyber Resiliency Engineering Framework. In *MITRE CORP BEDFORD MA* (Issue September).

http://www.mitre.org/work/tech_papers/2012/11_4436/%5Cnpapers2://publication/uuid/F03D9287-780F-4B61-AC47-E77BEDC3F939

Borky, J. M., & Bradley, T. H. (2019). Protecting Information with Cybersecurity. In *Effective Model-Based Systems Engineering*. Springer, Cham. <https://doi.org/10.1007/978-3-319-95669-5>

Caralli, R. A., Allen, J. H., White, D. W., Young, L. R., Mehravari, N., & Curtis, P. D. (2016). CERT Resilience Management Model (CERT-RMM) Version 1.2. In *CERT Resilience Management Model (CERT-RMM) Version 1.2* (Issue February).

https://resources.sei.cmu.edu/asset_files/Handbook/2016_002_001_514462.pdf

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process. In *Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst* (Issue May).

https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

Carayannis, E. G., Grigoroudis, E., Rehman, S. S., & Samarakoon, N. (2021). Ambidextrous Cybersecurity: The Seven Pillars (7Ps) of Cyber Resilience. *IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT*, 68(1), 223–234.

<https://doi.org/10.1109/TEM.2019.2909909>PANDED) WE - Social Science Citation Index (SSCI)

Carías, J. F., Arrizabalaga, S., Labaka, L., & Hernantes, J. (2020). Cyber Resilience Progression Model. *APPLIED SCIENCES-BASEL*, 10(21), 1–32. <https://doi.org/10.3390/app10217393>

Carías, J. F., Arrizabalaga, S., Labaka, L., & Hernantes, J. (2021). Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs. *IEEE ACCESS*, 9, 80741–80762.

<https://doi.org/10.1109/ACCESS.2021.3085530>

Carías, J. F., Borges, M. R. S., Labaka, L., Arrizabalaga, S., & Hernantes, J. (2020). Systematic Approach to Cyber Resilience Operationalization in SMEs. *IEEE ACCESS*, 8, 174200–174221.

<https://doi.org/10.1109/ACCESS.2020.3026063>

Carías, J. F., Labaka, L., Sarriegi, J. M., & Hernantes, J. (2019). Defining a Cyber Resilience Investment Strategy in an Industrial Internet of Things Context. *SENSORS*, 19(1).

<https://doi.org/10.3390/s19010138>

Carías, J. F., Labaka, L., Sarriegi, J. M., & Hernantes, J. (2018). An Approach to the Modeling of Cyber Resilience Management. *Proceedings of 2018 GLOBAL INTERNET OF THINGS SUMMIT (GIOTS)*, 110–115. <https://doi.org/10.1109/GIOTS.2018.8534579>

Catteddu, D., & Hogben, G. (2009). Cloud Computing Security Risk Assessment. *Enisa, December*, 1–2.

Chandra, S., & Kumar, K. N. (2018). Exploring factors influencing organizational adoption of augmented reality in e-commerce: Empirical analysis using technology-organization-environment model. *Journal of Electronic Commerce Research*, 19(3), 237–265.

Checkpoint. (2021). Another cyber attack on NZ businesses - analysis _ RNZ. RNZ.

<https://www.rnz.co.nz/national/programmes/checkpoint/audio/2018811564/another-cyber-attack-on-nz-businesses-analysis>

Chen, P. Y., Kataria, G., & Krishnan, R. (2011). Correlated failures, diversification, and information security risk management. *MIS Quarterly: Management Information Systems*, 35(2), 397–422.

<https://doi.org/10.2307/23044049>

Chiang, J. (2022). *Why is NZ lagging behind the world in cybersecurity?* Security Brief.

<https://securitybrief.co.nz/story/why-is-nz-lagging-behind-the-world-in-cybersecurity>

Christine, D., & Thinyane, M. (2020a). Cyber Resilience in Asia-Pacific - A Review of National Cybersecurity Strategies. *United Nations University*, 1–84.

Christine, D., & Thinyane, M. (2020b). Comparative Analysis of Cyber Resilience Strategy in Asia-Pacific Countries. *Proceedings of 18th International Conference on Dependable, Autonomic and Secure Computing, IEEE 18th International Conference on Pervasive Intelligence and Computing, IEEE 6th International Conference on Cloud and Big Data Computing and IEEE 5th Cybe*, 71–78. <https://doi.org/10.1109/DASC-PICom-CBDCCom-CyberSciTech49142.2020.00027>

CISA. (2016a). *CRR Supplemental Resource Guide - asset management* (Vol. 2).

<https://www.cisa.gov/publication/crr-supplemental-resource-guides>

CISA. (2016b). *CRR Supplemental Resource Guide - Configuration and Change Management* (Vol. 3). <https://www.cisa.gov/publication/crr-supplemental-resource-guides>

CISA. (2020a). *Cyber Resilience Review (Crr)*. Cybersecurity & Infrastructure Security Agency. <https://www.sei.cmu.edu/legal/request-permission-to-use-sei-material/cyber-resilience-review-usage->

CISA. (2020b). CYBER RESILIENCE REVIEW (CRR) Method Description and Self-Assessment User Guide. In *Carnegie Mellon University*.

<https://www.cisa.gov/uscrt/sites/default/files/c3vp/csc-crr-method-description-and-user-guide.pdf>

Cogburn, T. (2022). *What is Security Operations? Defined, Explained, and Trends*. Vation.

<https://www.vationventures.com/research-article/what-is-security-operations>

Collier, Z. A., Dimase, D., Walters, S., Tehranipoor, M. M., Lambert, J. H., & Linkov, I. (2014).

Cybersecurity standards: Managing risk and creating resilience. *Computer*, 47(9), 70–76.

<https://doi.org/10.1109/MC.2013.448>

Curtis, B., Hefley, B., & Miller, S. (2009). *People Capability Maturity Model (P-CMM) Version 2.0, Second Edition* (Issue July). [https://doi.org/Report CMU/SRI-2001-MM-001](https://doi.org/Report%20CMU/SRI-2001-MM-001)

Curtis, P. D., Mehravari, N., & Stevens, J. F. (2015). Cybersecurity Capability Maturity Model for Information Technology Services (C2M2 for IT Services), Version 1.0. In *Defense Technical Information Center* (Issue April). <https://apps.dtic.mil/sti/pdfs/AD1026943.pdf>

De Bruin, R., & Von Solms, S. H. (2016). Cybersecurity Governance: How can we measure it? *Proceedings of 2016 IST-Africa Conference, IST-Africa 2016*, 1–9.

<https://doi.org/10.1109/ISTAFRICA.2016.7530578>

- DeMarco, J. V. (2018). An approach to minimizing legal and reputational risk in Red Team hacking exercises. *COMPUTER LAW & SECURITY REVIEW*, 34(4), 908–911.
<https://doi.org/10.1016/j.clsr.2018.05.033>
- Drivas, G., Chatzopoulou, A., Maglaras, L., Lambrinoudakis, C., Cook, A., & Janicke, H. (2020). A NIS Directive Compliant Cybersecurity Maturity Assessment Framework. *Proceedings of 2020 IEEE 44th Annual Computers, Software, and Applications Conference, COMPSAC 2020*, 1641–1646.
<https://doi.org/10.1109/COMPSAC48688.2020.00-20>
- Dupont, B. (2019). The cyber-resilience of financial institutions: Significance and applicability. *Journal of Cybersecurity*, 5(1), 1–17. <https://doi.org/10.1093/cybsec/tyz013>
- Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and cybersecurity risk management. *Current Issues in Auditing*, 13(2), C1–C9. <https://doi.org/10.2308/ciia-52419>
- Ernst & Young. (2020). *How does security evolve from bolted on to built-in? EY Global Information Security Survey 2020*. <https://conferenceresources.fiba.net/wp-content/uploads/2020/10/EY-Global-Information-Security-Survey-2020.pdf>
- Estay, D. A. S. (2021). A system dynamics, epidemiological approach for high-level cyber-resilience to zero-day vulnerabilities. *JOURNAL OF SIMULATION*, 1–16.
<https://doi.org/10.1080/17477778.2021.1890533>
- Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, 86, 13–23.
<https://doi.org/10.1016/j.dss.2016.02.012>
- Financial Stability Board. (2018). *Cyber Lexicon* (Issue November). <https://www.fsb.org/wp-content/uploads/P121118-1.pdf>
- Fonseka, D. (2021). Ministry of Health abandoned cybersecurity system for Waikato and other DHBs due to budget issues. *Stuff*, 1–27.
<https://www.stuff.co.nz/business/125180968/ministry-of-health-abandoned-cybersecurity-system-for-waikato-and-other-dhbs-due-to-budget-issues>
- Foster, E. D., & Deardorff, A. (2017). Open Science Framework (OSF). *Journal of the Medical Library Association : JMLA*, 105(2), 203–206. <https://doi.org/10.5195/jmla.2017.88>
- Furnell, S., Fischer, P., & Finch, A. (2017). Can't get the staff? The growing need for cyber-security skills. *Computer Fraud and Security*, 2017(2), 5–10. [https://doi.org/10.1016/S1361-3723\(17\)30013-1](https://doi.org/10.1016/S1361-3723(17)30013-1)
- Gafic, M., Tjoa, S., & Kieseberg, P. (2022). A Novel Approach Integrating Design Thinking

Techniques in Cyber Exercise Development. *Proceedings of THE INTERNATIONAL CONFERENCE ON APPLIED CYBER SECURITY (ACS) 2021*, 378(ACS), 103–113.
https://doi.org/10.1007/978-3-030-95918-0_11

Gafic, M., Tjoa, S., Kieseberg, P., Hellwig, O., & Quirchmayr, G. (2021). Cyber Exercises in Computer Science Education. *Proceedings of THE 8TH INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS SECURITY AND PRIVACY (ICISSP)*, 404–411.
<https://doi.org/10.5220/0010845800003120>

Galinec, D., & Steingartner, W. (2018). Combining cybersecurity and cyber defense to achieve cyber resilience. *Proceedings of 2017 IEEE 14th International Scientific Conference on Informatics, INFORMATICS 2017 - Proceedings, 2018-Janua*, 87–93.
<https://doi.org/10.1109/INFORMATICS.2017.8327227>

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. *Risk Analysis*, 40(1), 183–199. <https://doi.org/10.1111/risa.12891>

Garcia-Perez, A., Sallos, M. P., & Tiwasing, P. (2021). Dimensions of cybersecurity performance and crisis response in critical infrastructure organisations: an intellectual capital perspective. *JOURNAL OF INTELLECTUAL CAPITAL*, 24(2), 465–486. <https://doi.org/10.1108/JIC-06-2021-0166>

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A Cyber-Security Culture Framework for Assessing Organization Readiness. *Journal of Computer Information Systems*, 62(3), 452–462. <https://doi.org/10.1080/08874417.2020.1845583>

Goldman, K. D., & Schmalz, K. J. (2004). The Matrix Method of literature reviews. *Health Promotion Practice*, 5(1), 5–7. <https://doi.org/10.1177/1524839903258885>

Gregor, S., & Hevner, A. (2013). Positioning and Presenting Design Science Research for Maximum Impact. *MIS Quarterly*, 37(2), 337–355. <https://www.jstor.org/stable/43825912>

Gutierrez, A., Boukrami, E., & Lumsden, R. (2015). Technological, organisational and environmental factors influencing managers' decision to adopt cloud computing in the UK. *Journal of Enterprise Information Management*, 28(6), 788–807.
<https://doi.org/10.1108/JEIM-01-2015-0001>

Harris, M. A., & Martin, R. (2021). Promoting Cybersecurity Compliance. *Research Anthology on Privatizing and Securing Data*, 1990–2007. <https://doi.org/10.4018/978-1-7998-8954-0.ch097>

Harrop, W., & Matteson, A. (2013). Cyber resilience: a review of critical national infrastructure and

- cyber security protection measures applied in the UK and USA. *Journal of Business Continuity & Emergency Planning*, 7(2), 149–162. https://doi.org/10.1057/9781137455550_10
- Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things*, 11, 1–9. <https://doi.org/10.1016/j.iot.2020.100204>
- Hevner, A., & Chatterjee, S. (2010). Design Science Research in Information Systems. In *Design Research in Information Systems*. Springer, Boston, MA. https://doi.org/10.1007/978-1-4419-5653-8_2
- Hevner, A., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, 28(1), 75–105. <https://www.jstor.org/stable/25148625>
- Homeland Security. (2014). *CRR-NIST CSF Crosswalk*. <https://www.hsdl.org/?view&did=767854>
- Hopcraft, R., Tam, K., Dorje Palbar Misas, J., Moara-Nkwe, K., & Jones, K. (2022). Developing a maritime cyber safety culture: Improving safety of operations. *Maritime Technology and Research*, 5(1), 258750. <https://doi.org/10.33175/mtr.2023.258750>
- Huang, K., & Pearlson, K. (2019). For what technology can't fix: Building a model of organizational cybersecurity culture. *Proceedings of the 52nd Hawaii International Conference on System Sciences, 2019-Janua*, 6398–6407. <https://doi.org/10.24251/hicss.2019.769>
- Huang, Y., Huang, L., & Zhu, Q. (2022). Reinforcement Learning for feedback-enabled cyber resilience. *Annual Reviews in Control*, 53(January), 273–295. <https://doi.org/10.1016/j.arcontrol.2022.01.001>
- Hunt, T. (2023). Information gleaned in NZ government contractor hack released on the dark web. *Stuff*. <https://www.stuff.co.nz/dominion-post/wellington/130996485/information-gleaned-in-nz-government-contractor-hack-released-on-the-dark-web>
- Iivari, J. (2015). Distinguishing and contrasting two strategies for design science research. *European Journal of Information Systems*, 24(1), 107–115. <https://doi.org/10.1057/ejis.2013.35>
- Iovan, S., & Iovan, A.-A. (2016). From Cyber Threats To Cyber-Crime. *Journal of Information Systems & Operations Management*, 425–434. <http://www.rebe.rau.ro/RePEc/rau/jisomg/WI16/JISOM-WI16-A15.pdf>
- ISACA. (2018). ISACA glossary. In *ISACA* (Vol. 4, Issue 1, pp. 88–100). <https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/glossary/glossary.pdf>
- Jensen, M. S. (2019). Cyber resilience, sectoral principle and responsibility placement - Nordic experience. *INTERNASJONAL POLITIKK*, 77(3), 266–277.

<https://doi.org/10.23865/intpol.v77.1369>

- Joiner, K. F. (2017). How Australia can catch up to U.S. cyber resilience by understanding that cyber survivability test and evaluation drives defense investment. *Information Security Journal*, 26(2), 74–84. <https://doi.org/10.1080/19393555.2017.1293198>
- Karjalainen, M., & Kokkonen, T. (2020). Comprehensive Cyber Arena; The Next Generation Cyber Range. *Proceedings of 2020 IEEE EUROPEAN SYMPOSIUM ON SECURITY AND PRIVACY WORKSHOPS (EUROS&PW 2020), 5th IEEE European Symposium on Security and Privacy (IEEE Euro S and P)*, 11–16. <https://doi.org/10.1109/EuroSPW51379.2020.00011>
- Katsumata, P., Hemenway, J., & Gavins, W. (2010). Cybersecurity risk management. *Proceedings of IEEE Military Communications Conference MILCOM*, 890–895. <https://doi.org/10.1109/MILCOM.2010.5680181>
- Keall, C. (2023). Ransomware attacks : Privacy Commissioner plans investigation as Justice , Health hit. *NZHerald.Co.Nz*, 3–8. <https://www.nzherald.co.nz/business/spreading-cyberattacks-privacy-commissioner-opening-investigation-into-wellingtons-mercury-it/SL5KSANTGBHCNEWC7G77VKU3XU/>
- Khan, O., & Estay, D. A. S. (2015). Supply Chain Cyber-Resilience: Creating an Agenda for Future Research. *TECHNOLOGY INNOVATION MANAGEMENT REVIEW*, 5(4), 6–12. <https://doi.org/10.22215/timreview885>
- King, S., & Ockels, C. (2009). *Defining Small Business Innovation* (Issue March, pp. 1–8). <https://www.mbie.govt.nz/assets/defining-small-business.pdf>
- Kissel, R. (2014). *Small business information security: the fundamentals* (Vol. 1). No. NIST Internal or Interagency Report (NISTIR) 7621 Rev. 1 (Draft). <https://csrc.nist.gov/publications/detail/nistir/7621/archive/2009-10-01>
- Knapp, E. (2011). Monitoring Enclaves. *Industrial Network Security*, 0, 215–247. <https://doi.org/10.1016/B978-1-59749-645-2.00009-4>
- Kosutic, D., & Pigni, F. (2022). Cybersecurity: investing for competitive outcomes. *Journal of Business Strategy*, 43(1), 28–36. <https://doi.org/10.1108/JBS-06-2020-0116>
- Kott, Alexander, & Linkov, I. (2019). Cyber Resilience of Systems and Networks. In A Kott & I. Linkov (Eds.), *Cyber Resilience of Systems and Networks*. Springer International Publishing. <https://doi.org/10.1007/978-3-319-77492-3>
- Krumay, B., Bernroider, E. W. N., & Walser, R. (2018). Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST

- Cybersecurity Framework. *Proceedings of Nordic Conference on Secure IT Systems*, 11252 LNCS, 369–384. https://doi.org/10.1007/978-3-030-03638-6_23
- Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers and Security*, 105, 102248. <https://doi.org/10.1016/j.cose.2021.102248>
- Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45(February 2018), 13–24. <https://doi.org/10.1016/j.ijinfomgt.2018.10.017>
- Linkov, I., Eisenberg, D. A., Bates, M. E., Chang, D., Convertino, M., Allen, J. H., Flynn, S. E., & Seager, T. P. (2013). Measurable Resilience for Actionable Policy. *Environmental Science & Technology*, 47, 10108–10110. <https://doi.org/10.1021/es403443n>
- Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J. H., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions*, 33(4), 471–476. <https://doi.org/10.1007/s10669-013-9485-y>
- Linkov, I., & Kott, A. (2018). Fundamental Concepts of Cyber Resilience: Introduction and Overview. In A. Kott & I. Linkov (Eds.), *Cyber Resilience of Systems and Networks*. (1st ed., pp. 1–25). Springer, Cham. <https://doi.org/10.1007/978-3-319-77492-3>
- Low, C. (2006). A framework for the governance of social enterprise. *International Journal of Social Economics*, 33(5–6), 376–385. <https://doi.org/10.1108/03068290610660652>
- MBIE. (2019). *Small business*. Ministry of Business Innovation & Employment. <https://www.mbie.govt.nz/business-and-employment/business/support-for-business/small-business/>
- Morakanyane, R., Grace, A., & O'Reilly, P. (2017). Conceptualizing digital transformation in business organizations: A systematic review of literature. *Proceedings of 30th Bled EConference: Digital Transformation - From Connecting Things to Transforming Our Lives, BLED 2017*, 427–444. <https://doi.org/10.18690/978-961-286-043-1.30>
- Mueller, M. (2017). Is cybersecurity eating internet governance? Causes and consequences of alternative framings. *Digital Policy, Regulation and Governance*, 19(6), 415–428. <https://doi.org/10.1108/DPRG-05-2017-0025>
- Muneer, F. (2022). Cybersecurity capability maturity model. In *U.S Department of Energy: Vol. 2.1*. [https://www.energy.gov/sites/default/files/2022-06/C2M2 Version 2.1 June 2022.pdf](https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf)

- Musa, N. (2018). A Conceptual Framework of IT Security Governance and Internal Controls. In K. A. Z. Abidin, M. Mohd, & Z. Shukur (Eds.), *Proceedings of THE 2018 CYBER RESILIENCE CONFERENCE* (Issue Cyber Resilience Conference (CRC), pp. 1–4). IEEE.
<https://doi.org/10.1109/CR.2018.8626831>
- Nagle, T., Doyle, C., Sammon, D., & Mohammed Alhassan, I. (2020). The Research Method we Need or Deserve? A Literature Review of the Design Science Research Landscape. *Communications of the Association for Information Systems*.
<https://doi.org/https://doi.org/10.31219/osf.io/yjbd7>
- NCSC. (2018). *INCIDENT MANAGEMENT*. <https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Incident-Management-Be-Resilient-Be-Prepared.pdf>
- NCSC. (2020). *New Zealand Information Security Manual v.3.4* (Issue 00).
<https://www.gcsb.govt.nz/our-work/national-cyber-security-centre-ncsc/new-zealand-information-security-manual-nzism/>
- NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*.
<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf%0Ahttps://doi.org/10.6028/NIST.CSWP.04162018>
- North, J., & Pascoe, R. (2016). Cyber security and resilience -- it's all about governance. *Governance Directions*, 68(3), 146–151. <https://doi.org/10.3316/ielapa.003855469276044>
- Nunamaker, J. F., Briggs, R. O., Derrick, D. C., & Schwabe, G. (2015). The Last Research Mile: Achieving Both Rigor and Relevance in Information Systems Research. *Journal of Management Information Systems*, 32(3), 10–47.
<https://doi.org/10.1080/07421222.2015.1094961>
- Executive order 13636: Improving critical infrastructure cybersecurity, Pub. L. No. Executive order 13636, 78 Cybersecurity: Executive Order 13636 and the Critical Infrastructure Framework 11739 (2013). <https://www.govinfo.gov/content/pkg/FR-2013-02-19/pdf/2013-03915.pdf>
- Onishchenko, O., Shumilova, K., Volyanskyy, S., Volyanskaya, Y., & Volianskyi, Y. (2022). Ensuring Cyber Resilience of Ship Information Systems. *INTERNATIONAL JOURNAL ON MARINE NAVIGATION AND SAFETY OF SEA TRANSPORTATION*, 16(1), 43–50.
<https://doi.org/10.12716/1001.16.01.04>
- Onwubiko, C. (2020a). CyberOps: Situational Awareness in Cybersecurity Operations. *International Journal on Cyber Situational Awareness*, 5(1), 82–107.
<https://doi.org/10.22619/ijcsa.2020.100134>

- Onwubiko, C. (2015). Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy. *Proceedings of 2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment*, 1–2.
<https://doi.org/10.1109/CyberSA.2015.7166125>
- Onwubiko, C. (2020b). Focusing on the Recovery Aspects of Cyber Resilience. *Proceedings of 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment*, 1–13. <https://doi.org/10.1109/CyberSA49311.2020.9139685>
- Paradis, S., Benaskeur, A., Oxenham, M., & Cutler, P. (2005). Threat evaluation and weapons allocation in network-centric warfare. *Proceedings of 2005 7th International Conference on Information Fusion*, 2, 1078–1085. <https://doi.org/10.1109/ICIF.2005.1591977>
- Pawar, S., & Palivela, D. H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). *International Journal of Information Management Data Insights*, 2(1), 100080. <https://doi.org/10.1016/j.jjime.2022.100080>
- Peffer, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3), 45–77. <https://doi.org/10.2753/MIS0742-1222240302>
- Pernice, I. (2018). Global cybersecurity governance: A constitutionalist analysis. *Global Constitutionalism*, 7(1), 112–141. <https://doi.org/10.1017/S2045381718000023>
- Pupillo, L. (2018). EU Cybersecurity and the Paradox of Progress. *CEPS Policy Insight*, 06, 1–10.
- Reserve Bank of New Zealand. (2022). *Improving cyber resilience for regulated entities*. Reserve Bank of New Zealand. <https://www.rbnz.govt.nz/regulation-and-supervision/cross-sector-oversight/improving-cyber-resilience-for-regular-entities>
- Roberts, N. (2021). *Business size categories in New Zealand : Definitions and why they matter*. MYOB. <https://www.myob.com/nz/blog/what-sized-business-are-you-2/>
- Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. *National Institute of Standards and Technology*, 2, 310.
- Ruefle, R., Wyk, K. Van, & Tomic, L. (2013). *New Zealand Security Incident Management Guide for Computer Security Incident Response Teams (CSIRTs)*.
<http://www.ncsc.govt.nz/resources.html>
- Ruffini, F. A. J., Boer, H., & Riemsdijk, M. J. van. (2000). Organisation design in operations management. *International Journal of Operations & Production Management*, 20(7), 860–

- Samonas, S., Dhillon, G., & Almusharraf, A. (2020). Stakeholder perceptions of information security policy: Analyzing personal constructs. *International Journal of Information Management*, 50(April 2019), 144–154. <https://doi.org/10.1016/j.ijinfomgt.2019.04.011>
- Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International Cybersecurity Law Review*, 3(1), 7–34. <https://doi.org/10.1365/s43439-021-00045-4>
- Shackleton, T. (2021). *When Too Much Cyber Security Spending Still Isn't Enough: And what to do about it in 2022*. Six Degrees. <https://www.6dg.co.uk/blog/cyber-security-spending/>
- Spremić, M., & Šimunic, A. (2018). Cyber security challenges in digital economy. *Proceedings of the World Congress on Engineering 2018*, 1, 2–7.
- Spruit, M., & Roeling, M. (2014). ISFAM: The information security focus area maturity model. *Proceedings of 22nd European Conference on Information Systems*, 0–15. <https://core.ac.uk/download/pdf/301362294.pdf>
- Spruit, M., & Slot, G. (2017). ISFAM 2.0: Revisiting the information security assessment model. *Security Risks: Assessment, Management and Current Challenges, February*, 87–108. https://www.researchgate.net/publication/321547446_ISFAM_20_Revisiting_the_information_security_assessment_model
- Statistics New Zealand. (2022). *New Zealand Business Demography Statistics: At February 2012 - Statistics New Zealand*. Stats NZ. http://www.stats.govt.nz/browse_for_stats/businesses/business_characteristics/BusinessDemographyStatistics_HOTPFeb12.aspx
- Tam, T., Rao, A., & Hall, J. (2021). The good, the bad and the missing: A Narrative review of cybersecurity implications for Australian small businesses. *COMPUTERS & SECURITY*, 109, 102385. <https://doi.org/10.1016/j.cose.2021.102385>
- The National Academy of Sciences. (2012). *Disaster Resilience: A National Imperative*. www.nap.edu
- Tiong Tan, K. S., Hoong Lee, A. S., & Min, C. T. (2021). Studying The Perception of Using Visualization Dashboard to Measure Cybersecurity Maturity Stage. *Proceedings of 7th International Conference on Research and Innovation in Information Systems*, 1–6. <https://doi.org/10.1109/ICRIIS53035.2021.9617069>
- Tsen, E., Ko, R. K. L., & Slapnicar, S. (2022). An exploratory study of organizational cyber resilience,

- its precursors and outcomes. *Journal of Organizational Computing and Electronic Commerce*, 32(2), 153–174. <https://doi.org/10.1080/10919392.2022.2068906>
- U. S. Small Business Administration, 1 (2022). <https://www.sba.gov/document/support-table-size-standards>
- van de Poel, I. (2020). Core Values and Value Conflicts in Cybersecurity: Beyond Privacy Versus Security. *International Library of Ethics, Law and Technology*, 21, 45–71. https://doi.org/10.1007/978-3-030-29053-5_3
- van der Kleij, R., & Leukfeldt, R. (2020). Cyber Resilient Behavior: Integrating Human Behavioral Models and Resilience Engineering Capabilities into Cyber Security. *Proceedings of ADVANCES IN HUMAN FACTORS IN CYBERSECURITY 2019*, 960(10th AHFE International Conference on Human Factors in Cybersecurity), 16–27. https://doi.org/10.1007/978-3-030-20488-4_2
- van Haastrecht, M., Golpur, G., Tzismadia, G., Kab, R., Priboi, C., David, D., Răcățăian, A., Brinkhuis, M., & Spruit, M. (2021). A shared cyber threat intelligence solution for smes. *Electronics*, 10(23), 1–21. <https://doi.org/10.3390/electronics10232913>
- Venable, J., Pries-Heje, J., & Baskerville, R. (2016). FEDS: A Framework for Evaluation in Design Science Research. *European Journal of Information Systems*, 25(1), 77–89. <https://doi.org/10.1057/ejis.2014.36>
- von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security*, 26(1), 2–9. <https://doi.org/10.1108/ICS-04-2017-0025>
- Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, 26(2), xiii–xxiii. <https://doi.org/10.1.1.104.6570>
- Williams, P., & Manheke, R. J. (2010). Small Business - A Cyber Resilience Vulnerability. *Proceedings of International Cyber Resilience Conference, August*, 112–119. <http://ro.ecu.edu.au/icr/14>
- Wong, L.-W., Lee, V.-H., Tan, G. W.-H., Ooi, K.-B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *INTERNATIONAL JOURNAL OF INFORMATION MANAGEMENT*, 66, 102520. <https://doi.org/10.1016/j.ijinfomgt.2022.102520>
- Yigit Ozkan, B. (2022). Cybersecurity Maturity Assessment and Standardisation [Utrecht University]. In *Doctoral dissertation, Utrecht University*. <https://doi.org/10.33540/869>
- Yusif, S., & Hafeez-Baig, A. (2021). A Conceptual Model for Cybersecurity Governance. *Journal of Applied Security Research*, 16(4), 490–513. <https://doi.org/10.1080/19361610.2021.1918995>

- Zemba, V., Wells, E. M., Wood, M. D., Trump, B. D., Boyle, B., Blue, S., Cato, C., & Linkov, I. (2019). Defining, measuring, and enhancing resilience for small groups. *Safety Science*, 120(April), 603–616. <https://doi.org/10.1016/j.ssci.2019.07.042>
- Zhang, A., Collins, R., & O'Connor-Close, C. (2020). Cyber incident cost estimates and the importance of building resilience. In *Reserve Bank of New Zealand Bulletin* (Vol. 84, Issue 2). <http://libaccess.mcmaster.ca/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=142844314&site=ehost-live&scope=site>
- Zwikael, O. (2008). Top management involvement in project management: Exclusive support practices for different project scenarios. In *Proceedings of International Journal of Managing Projects in Business* (Vol. 1, Issue 3, pp. 387–403). <https://doi.org/10.1108/17538370810883837>
- Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, 62(1), 82–97. <https://doi.org/10.1080/08874417.2020.1712269>