



Australian
National
University



TECH POLICY
DESIGN CENTRE

Australian Telecommunications Sector Resilience Profile

Keeping Australia connected in an uncertain world

SEPTEMBER 2024



About the Tech Policy Design Centre

The Tech Policy Design Centre (TPDC) is a nonpartisan, independent research and education organisation at the Australian National University. TPDC's mission is to shape technology for the long-term benefit of humanity. We work to mature the tech-governance ecosystem in collaboration with industry, government, civil society, and academia.

Independence Statement

Our work is made possible by the generous support of external funders from government, industry, and civil society philanthropy. This project was funded by the Department of Infrastructure, Transport, Regional Development, Communications and the Arts. Our research aligns with ANU's Statement on Academic Freedom. In all instances, TPDC retains full independence over our research and complete editorial discretion for outputs, reports, and recommendations.

Authors

Dr Huon Curtis, Senior Research Fellow, ANU Tech Policy Design Centre

Chloe Harpley, Project Manager, ANU Tech Policy Design Centre (on secondment from the Department of Infrastructure, Transport, Regional Development, Communications and the Arts)

Professor Johanna Weaver, Director, ANU Tech Policy Design Centre

Zoe Hawkins, Head of Policy Design, ANU Tech Policy Design Centre

James Jackson, Research Assistant, ANU Tech Policy Design Centre

Edited by Dr Cath Latham, Senior Fellow, ANU Tech Policy Design Centre

Acknowledgements

The TPDC acknowledges the Ngannawal and Ngambri people, who are the Traditional Owners of the land upon which this report was prepared. We pay our respects to their elders, past and present.

The TPDC thanks all who contributed to this work, including the project's Risk and Resilience Expert Panel, Alexander Osbourne, Cameron Scott, Carolyn Phiddian, Colin Muller, Craig Smith, Dave O'Loan, Dan Weis, David Haigh, Ebony Aitken, Elise Ball, Dr Gareth Downing, Gill Savage, Dr Holly Randell- Moon, Jamie Morse, Jason Duerden, Jeff Whitton, Professor Johanna Weaver (Chair) Kirsty McKinnon, Laurence Plant, Luke Coleman, Michelle Phillips, Min Livanidis, Narelle Clark, Dr Paul Barnes, Professor Ryan Ko, Stephen Farrugia, the Department of Infrastructure, Transport, Regional Development, Communications and the Arts, the Department of Home Affairs; and all of our Focus Group participants and attendees to the Risk and Resilience Symposium.

This report's cover image was created using the DALL-E artificial intelligence image generator.

Citation

Curtis H., Harpley C., Weaver J., Hawkins Z., Jackson J 2024 Australian Telecommunications Sector Resilience Profile: Keeping Australia Connected in an Uncertain World. ANU Tech Policy Design Centre.

Contact

Tech Policy Design Centre
5 Fellows Road, ANU College of Law
The Australian National University Canberra ACT 2601, Australia

techpolicydesign@anu.edu.au

CRICOS Provider: 00120C

Telecommunications Risk and Resilience Profile © 2024 by the ANU Tech Policy Design Centre is licensed under CC BY-SA 4.0. To view a copy of this license, visit <http://creativecommons.org/licenses/by-sa/4.0>



Australian
National
University



Table of contents

ABOUT THIS PROFILE	4
SECTION OVERVIEW	8
NEXT STEPS	11
1 PART 1 – TELECOMMUNICATIONS SECTOR RESILIENCE MATURITY ASSESSMENT	12
WHAT IS SECTOR RESILIENCE?	13
THE SECTOR RESILIENCE MATURITY MODEL	21
ASSESSMENT OF TELECOMMUNICATIONS SECTOR RESILIENCE MATURITY	24
2 PART 2 – EVIDENCE IN SUPPORT OF THE ASSESSMENT	40
STEP 1: DEFINING THE SECTOR	41
STEP 2: PREPARE AND ABSORB: SITUATIONAL AWARENESS OF THE RISK HORIZON	52
STEP 3: ADAPT, RESPOND, RECOVER: BUILDING CONSEQUENCE MANAGEMENT CAPABILITIES	86
STEP 4: LEARN AND TRANSFORM: LESSONS MANAGEMENT	93
APPENDICES	94
APPENDIX A. GLOSSARY	94
APPENDIX B. METHODOLOGIES	98
APPENDIX C. ASSUMPTIONS AND LIMITATIONS	109
APPENDIX D. SUGGESTED READING	111
APPENDIX E. RISK AND RESILIENCE EXPERT PANEL MEMBERS	112
APPENDIX F. STAKEHOLDERS CONSULTED	113
APPENDIX G. INDEX OF TABLES	114
APPENDIX H. INDEX OF FIGURES	115
APPENDIX I. BIBLIOGRAPHY	116

About this profile

ANU Tech Policy Design Centre (TPDC) was commissioned by the Department of Infrastructure, Transport, Regional Development, Communication and the Arts (DITRDCA) to profile the telecommunications sector to better understand the risk landscape and whole-of-sector resilience.

The resulting assessment and Profile detailed in this report provide a common language and the foundations for a shared vision and cooperative action. It should be revisited regularly to track progress and demonstrate the ongoing commitment to improving sector resilience.

By taking an all-hazards and sector-wide approach, this Profile has developed a framework to cement telecommunications' resilience in policy and operational practice.

The findings reflect consultations with 204 stakeholders from across the sector, representing all states, territories, and the federal government, plus representatives of dependent and interdependent sectors.¹ The evidence collected through these consultations shaped the whole-of-sector profile's resilience maturity assessment and development.

The final Profile and assessment were refined, shaped, and endorsed by a 26-member Risk and Resilience Expert Panel consisting of diverse practitioners with backgrounds in engineering, network architecture, climate change research, government, enterprise, and strategic policy.²

Building the Profile created forums among these key stakeholders, where large and small providers, regulators, and consumer representatives could share lessons around the same table. It provided the means to discuss and respond to complex scenarios, identify shared vulnerabilities, and outline a desired future state that would benefit all.

The consultative process led to the development of a shared vision and language of resilience, including a sector-specific lexicon to describe the risk factors (threats, threat sources, and vulnerabilities) and a Sector Resilience Maturity Model to guide cooperation, collaboration, and continuous improvement.

These insights, actions, and principles are not the final word, but rather lay the foundation for an ongoing, vital dialogue between government, industry, and communities in a critical sector.

¹ For full list of stakeholders consulted, see Appendix E.

² For a full list of members of the Risk and Resilience Expert Panel, see Appendix F.

Executive summary

Resilience in the telecommunications sector is foundational to Australia's collective well-being and progress. Connecting people via telecommunications has been a national priority since federation in 1901, when telephones and telegraph services were nationally funded infrastructure.³

Since then, the sector has transformed several times over. In the last 30 years, Australia's telecommunication sector has grown from landline services provided predominantly through one publicly owned company, Telecom⁴, to a thriving commercial landscape providing a range of phone and data services that support personal and business connectivity needs. This growth has happened against a backdrop of rapidly evolving technological advances. From landlines to dial-up internet, to mobile networks, and then smartphones, driving a huge increase in Australians' expectations and dependence on connectivity.

Telecommunications networks have been particularly tested over the past five years. In response to a range of disruptions, individual network providers have displayed remarkable strengths to rapidly restore services, adapt to evolving challenges, and maintain essential connectivity for millions of users. One example is the extraordinary efforts to maintain effective services during the COVID-19 pandemic, when capacity limits were stretched as millions of Australians shifted their work into their homes.

Today, telecommunications connectivity underpins nearly every aspect of our lives, from personal communications to global commerce, healthcare, and national security. It connects communities, empowers businesses, and drives innovation. In 2020, the Australian Government classed the telecommunications sector as critical national infrastructure. This marked a significant shift in its governance and underscored its importance to the nation's functioning, security, and prosperity.⁵

The telecommunications sector has been characterised by complex dynamics and competing interests. Industry players often view government regulation with suspicion, fearing it may distort the competitive landscape and impede market forces. There are knowledge gaps within government regarding the secular market trends in telecommunications. Regulatory frameworks often lag technological advancements and commercial realities, creating a disconnect between policy objectives and industry needs. At the same time, companies hesitate to cooperate with each other, fearing allegations of cartel behaviour, exclusive dealing, or misuse of market power. This has led to an environment where distrust and entrenched positions hinder sharing of information about critical vulnerabilities.

Telecommunications increasingly underpin interdependent critical sectors such as energy, finance, healthcare and transportation. Therefore, the consequences of ineffective policy and insufficient coordination ripple far beyond the industry itself, potentially impacting essential services and daily life for millions of Australians. From disruption to emergency services to impediments to economic activities, the stakes are higher than ever. As technologies like 5G, Internet of Things, artificial intelligence, and quantum computing reshape the digital landscape, interdependencies will deepen, and the sector will continue to face disruptions of increasing severity. Without a coordinated approach to sector-wide telecommunications resilience, the sector will struggle to fulfil its pivotal role in keeping Australians connected in an increasingly uncertain world.

Despite its national importance, the resilience of the Australian telecommunications sector has – until now – not been profiled at the sector-level. To date, it has been difficult to assess the resilience maturity of the whole telecommunications sector. This is due to different approaches by individual enterprises and levels of government, as well as a lack of a shared understanding of what resilience involves.

Here, we present a landmark initiative: Australia's first resilience profile for the telecommunications sector. This Profile represents a significant step forward in our national approach to critical infrastructure resilience. To build the Profile, the TPDC project team fostered and modelled collaboration among diverse stakeholders across the telecommunications sector. This process not only produced valuable insights, but demonstrated the feasibility and benefits of coordinated action.

3 Telstra Corporation Limited, *Submission to Public inquiry to make final access determinations for the declared fixed line services, Section 3A Historical Background*, 2011, <https://www.accc.gov.au/system/files/Schedule%20A.3%20of%20Telstra%20public%20submission.pdf>

4 The Australian Government sold Telecom in 1997. See reference 1.

5 Department of Home Affairs 2020, *Security Legislation Amendment (Critical Infrastructure) Bill 2020*, <https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems>

The Profile provides an evidence base for future policy and decision-making. As there was no pre-existing methodology, TPDC developed the Sector Resilience Maturity Model⁶ to assess sector-wide telecommunications resilience. Companion profiling tools capture the dynamism of the risk horizon, including its threats and vulnerabilities and the consequences of disruption.

By applying evidence collected over the life of this project to the Sector Resilience Maturity Model, TPDC assessed that the resilience maturity of the Australian telecommunications sector is ‘Developing (2)’, a score of two on a five-point scale.⁷ This indicates that basic resilience measures are in place, including initial efforts to coordinate sector-wide. The Model assesses the resilience maturity of the sector as a whole, including providers of services and assets, and governments at local, state and territory, and federal levels. It is not an assessment of the resilience of individual enterprises.

It is not surprising that Australia’s telecommunications sector is still developing resilience. Until now, the sector has lacked a well-defined framework for resilience, encompassing its regulatory scope and policy implications. Ambiguity results in inefficient resource allocation and missed opportunities for improvements.

The evidence presented across the Profile suggests that a more systematic approach is needed to capture, analyse, and apply lessons from past events to improve future performance.

This Profile clarifies resilience in the telecommunications context. It outlines guiding principles for policy, and identifies capabilities that, when developed, will improve resource allocation across the sector. This will improve coordination and clarify roles and responsibilities for all stakeholders, including government agencies, telecommunications providers, interdependent sectors, and communities. Combined, this will significantly and progressively mature sector-wide resilience.

This Profile provides a benchmark of current maturity of sector resilience. More importantly, it establishes a shared vision and ambition for sector-wide telecommunications resilience. It is an invitation and a roadmap to enhance the resilience of this critical sector on which all Australians depend every day.

6 An overview of the Sector Resilience Maturity Model is available in Part 1, page 20.

7 A detailed account of the assessment is available in part one of this report. Evidence supporting the assessment is available in part 2 of this report.

Key findings

1

Resilience is an emergent concept. No pre-existing fit-for-purpose methodologies existed to profile resilience at the sector-level.

2

To build this Profile, TPDC developed a conceptual framework for defining and assessing sector resilience: the Sector Resilience Maturity Model.

3

The Sector Resilience Maturity Model outlines the principles, capabilities and resources needed to mature sector resilience in the face of uncertainty. The Model serves two purposes.

First: it articulates a **shared vision** of sector resilience.

Second: it provides a **method to assess** sector resilience maturity.

5

Assessed against the Sector Resilience Maturity Model, the Australian telecommunications sector is at the 'Developing (2)' level of resilience maturity.⁸ This level indicates that basic resilience measures are in place, including initial efforts to coordinate sector-wide.

4

While the Sector Resilience Maturity Model was developed to profile the telecommunications sector, its methodology could also be used to assess resilience maturity of other sectors.

6

Contributing to the overall telecommunications sector resilience maturity score are assessments of the sector's maturity against resilience principles, capabilities and resourcing.

Principles: the sector is at the developing (2) level. Individual organisations may be guided by social, economic, and environmental resilience principles, but these efforts are fragmented and not cohesively aligned across the sector.

Capabilities: the sector is at the developing (2) level. The sector is more mature when it comes to asset maintenance and infrastructure hardening, and significantly less mature in relation to other resilience capabilities, such as those relating to data, standardisation, cross-sector engagement, and consequence management.

Resourcing: the sector is at the developing (2) level. Some resources, such as physical assets and technological solutions, are dedicated to resilience, but significant gaps remain.

7

The Sector Resilience Maturity Model and the resulting assessment were developed by TPDC and endorsed by the project's 26-member Expert panel. Both the Model and the assessment are a synthesis of evidence gathered across a multi-stage research and engagement process from February 2023 to May 2024, with the participation of 204 stakeholders.

8

This Profile captures a point in time assessment and a benchmark of the current maturity of telecommunications sector resilience. It should be revisited regularly to measure progress.

9

Resilience in the Australian telecommunications sector will be significantly enhanced by the operationalisation of the shared vision articulated in the Sector Resilience Maturity Model. This Profile should, therefore, not be treated as a static document, but rather as a roadmap for future cooperation.

⁸ Based on evidence collected for 2023-2024.

Section overview

Part 1: Sector Resilience Maturity Assessment

This part defines sector resilience, introduces the Sector Resilience Maturity Model, and applies that Model to the telecommunications sector to produce a maturity assessment.

What is resilience?

This section presents a comprehensive definition of resilience in the telecommunications sector that emphasises the sector's ability to sustain performance in the face of uncertainty. It recognises the need to develop capacities to manage the phases of disruption: to prepare, absorb, adapt, respond, recover, learn, and transform. Sector resilience requires sophisticated and dynamic capabilities in lessons management, consequence management, and risk management.

The Sector Resilience Maturity Model

There was no pre-existing fit-for-purpose framework to evaluate sector-level resilience. So TPDC developed the Sector Resilience Maturity Model (SRMM), comprising three key components:

- **Resilience principles:** the foundational vision steering resilience efforts.
- **Resilience capabilities:** the specific actions that enable the sector to manage disruptions.
- **Resilience resources:** the necessary assets to support these efforts.

The SSRM establishes these five maturity levels:

1. **Initial:** Resilience practices are unstructured and reactive across the sector.
2. **Developing:** Basic resilience measures are established, including initial sectoral coordination efforts.
3. **Defined:** Resilience processes are well-defined and documented across the sector.
4. **Managed:** Resilience practices are systematically integrated and applied consistently across the sector.
5. **Optimised:** Resilience is continuously improved through proactive learning, innovation, and transformation.

Assessment of telecommunications sector resilience maturity

This section applies the evidence collected over the project's life to the telecommunication sector's resilience. It concludes that the telecommunications sector is at a 'Developing (2)' level of resilience maturity. This indicates that basic resilience measures are in place, including initial sector-wide coordination efforts.

Part 2: Evidence in support of the Sector Resilience Maturity Assessment

This part presents the evidence collected by TPDC during 2023-2024, which informed the development of the SRRM and the resilience maturity assessment of the telecommunications sector.

Defining the sector

The section defines the telecommunications sector as a complex socio-technical system. It clarifies the sector's purpose, assets, services, entities, stakeholders, performance, and value. A broad definition reinforces the need for a shared vision, and provides the rationale for developing a sector-specific resilience maturity model and assessment.

Prepare and absorb: Situational awareness of the risk landscape and risk management

This section develops standardised terminology and frameworks for identifying and categorising threats and vulnerabilities, allowing for greater precision in discussions across different stakeholder groups.

- **Threats:** The evidence shows that the Australian telecommunications sector is constantly challenged by a dynamic threat landscape that can significantly impact service continuity. Threats have been identified across 6 threat categories: physical, cyber and technological, climate and environmental, economic, regulatory, and supply chain.
- **Threat sources:** The evidence identifies the source of threats to the sector, including both malicious actors and non-malicious sources.
- **Vulnerabilities:** The evidence suggests a persistent concern across project stakeholders of the inability at the sector-level to integrate lessons from disruption. Sector-level vulnerabilities arise from weaknesses in enterprise and government approaches. Without proper incentives and procedures, the sector becomes susceptible to vulnerabilities, potentially impacting interconnected sectors and socio-economic functions.

The evidence presented in this section can be used by enterprises and governments to enhance situational awareness, ultimately building greater capacities to manage disruption.

Adapt, respond, recover: Consequence and its management

This section acknowledges that disruptions in telecommunications can have wide-ranging consequences, making effective consequence management crucial for maintaining public safety, economic functions, and service reliability.

This section provides evidence of weaknesses in consequence management capabilities in the Australian telecommunications sector. These weaknesses have been identified in communicating crisis information to the public across various scenarios. Deficiencies exist in the visibility of asset-level information and bidirectional information sharing.

At the sector-level, improved consequence management requires coordinated efforts among all stakeholders, including providers, regulators, interdependent sectors, and end-users. This involves sector-wide information sharing during crises to guide stakeholder actions during disruptions, improving cooperation and coordination, and strengthening innovation.

Enterprises and governments can use the evidence in this section to improve consequence management. It includes measures to ensure business continuity, such as incident response protocols, crisis communications, and recovery plans, to ensure that critical functions are rapidly restored.

Learn and transform: Lessons management

This section recognises that disruptions will occur, so learning lessons from the past isn't just helpful; it's critical for maturing the sector and preparing for the unforeseen.

The evidence presented in this section, and across the Profile, suggests that a more structured approach is needed to capture, analyse, and apply lessons from past events to improve future performance.

The section concludes with a recognition that sector-level learning is a collective effort that can reshape the entire telecommunications landscape. It creates a shared vision, informs practical regulatory frameworks, guides investments, and fosters collaborative innovation.

An overview of the steps taken, tools developed, and findings of this Profile are depicted in Figure 1.

Figure 1. Profiling resilience in the Australian telecommunications sector

Steps taken to build the profile	Profiling tools	Findings and/or assessment
What is Resilience? Defining sector-wide resilience and its relationship to risk	Understanding what principles, capabilities and resources underpin effective resilience at the sector level.	Building resilience in the Australian telecommunications sector requires maturing capacities across all phases of disruption management – prepare, absorb, adapt, respond, recover, lean and transform.
Defining the sector Who are the stakeholders involved?	Determining who is involved in the sector to understand roles and responsibilities in telecommunications resilience. This includes stakeholders across industry, government, society.	The Australian telecommunications sector is a complex socio-technical system of entities, stakeholders and assets that enables communication to the intended recipient through the transmission, reception and/or delivery of information or data.
Understanding the Risk Horizon Risk management: Developing situational awareness of the risk horizon and preparing for unexpected disruptions	Threats: TPDC Threat Taxonomy Threat sources: TPDC Threat Source Categories Vulnerabilities: TPDC Vulnerability Categories	A wide range of threats, threat sources and vulnerabilities contribute to the risk horizon for the Australian telecommunications sector. Resilience requires sector-wide monitoring and preparation for inevitable disruptions (situational awareness), ideally in near realtime.
Understanding how the sector adapts, responds & recovers Consequence management: Building capabilities to ensure services continue when disruptions occur	Mechanisms for information-sharing and co-ordination across the sector TPDC Consequence Management Analysis	There is an immediate need for greater information-sharing and coordination between public and private sector stakeholders. A greater focus by government on resilience policy & regulatory settings would enhance sector consequence management.
Assessing the sector's resilience and mechanisms for maturing it Lessons management: Assessing and maturing sector resilience by learning and transforming	Capacity to manage disruptions – assessed against resilience capabilities, principles and resources TPDC Sector Resilience Maturity Model Dependent on the sector stakeholders having: <ul style="list-style-type: none"> • a shared vision and shared responsibility for resilience • a common understanding of resilience maturity 	The Australian telecommunications sector is currently at a ' developing ' level of resilience maturity (level 2 of 5). Maturing sector resilience will require implementing a shared vision among stakeholders through cooperation and shared responsibility.

Next steps

This Profile highlights the need to sharpen responses and continue to build resilience to large-scale telecommunications disruptions. This includes developing and enhancing coordination, cooperation, and innovation mechanisms among the various stakeholders that define the sector. To build on this Profile, we recommend the following steps.

For industry:

Consider that commercially differentiated responses to resilience already in place should be better aligned and coordinated through the sector as a whole. While these different approaches may be ‘market-leading’, many have been developed and established by a single enterprise acting as a ‘lone planner’. Though these approaches are effective in maintaining an individual provider’s services through disturbances in performance, issues caused by large-scale disruptions require both preparation and responses at a sector-level.⁹

Where industry self-assesses its resilience maturity to be ahead of other stakeholders in the sector, it is an opportunity for those enterprises to share lessons learned, and guide whole-of-sector improvement.

For the Australian Government:

There is an opportunity to significantly advance Australia’s telecommunications sector’s maturity by developing and implementing clear and coherent resilience policy settings that guide industry. The assessment in this Profile that the sector is at a ‘developing’ level of maturity largely reflects the early stage of resilience integration in Australian federal policies. Evidence collected during this project strongly suggests that policy settings could better support and incentivise the sector to develop and mature its resilience.

Australian Government policies should, where possible, build upon existing approaches developed by industry, state and territory governments, and academia, to mature resilience at the sector-level. These policy settings should be supported by regulatory frameworks designed to inform meaningful change and avoid excessive reporting requirements.

For all telecommunications sector stakeholders:

Work together to systematically integrate, consistently apply, and continuously improve resilience approaches. Through collective responsibility and coordinated approaches, resilience for the sector becomes greater than the sum of its parts.

Developing a comprehensive theory of change by all stakeholders is crucial to guide the implementation of findings and mature resilience capacities. Such a framework should outline a strategic approach to change management, detailing how deficiencies can be addressed, and beneficial practices more widely adopted. It should incorporate mechanisms for building capability, increasing resilience resources, and promoting a culture of continuous improvement within the sector. The theory of change should also consider the evolving nature of the risk horizon and the need for flexible, responsive systems. A theory of change will help to link the capabilities identified in the maturity model to implementation.

Creating detailed playbooks by government and industry for consequence management is essential. These playbooks should provide structured, actionable guidance for responding to various scenarios identified in this Profile. They should outline clear protocols for coordination, decision-making, and resource allocation during times of disruption, building on current mechanisms, ensuring that the sector can better manage and mitigate the consequences of disruptive events. These playbooks should be designed to be easily updated, allowing for the incorporation of new insights and lessons learned from real-world applications.

9 Phillips, B & Landahl, M 2020, *Business Continuity Planning: Increasing Workplace Resilience to Disasters*, ScienceDirect, <https://doi.org/10.1016/C2017-0-00385-3>

1

Part 1 – Telecommunications Sector Resilience Maturity Assessment

In this section:

What is sector resilience

Overview of the Sector Resilience Maturity Model

Assessment of current sector maturity

- Resilience principles
- Resilience capabilities
- Resilience resources

What is sector resilience?

“Resilience is an emergent systems concept – it only appears via the shadow it casts. You can only really discern resilience via its absence: when there are no surprises, you may be resilient. If there are disruptions, you may not be. Resilience is the ability to sustain continuity of functions while recovering. Resilient organisations are able to increase the capacities required to function with a high degree of reliability in the face of disruption.”¹⁰

In recent years, there has been a growing emphasis on the concept of resilience to enhance the capacity of sectors to withstand, adapt to, and recover from disruptive events. General definitions of resilience exist but need to be contextualised in relation to specific sectors, particularly where commercial interests intersect with society, the economy and national security. In compiling this Profile, TPDC developed the definition of sector resilience described in this section. Notably, risk remains important; however, it is reframed as an element of resilience, rather than a standalone concept.

Traditionally, continuity of service at the sector-level has been viewed through a risk paradigm, involving risk identification, evaluation and treatment.¹¹ While the concept of ‘risk’ has been well-established and widely used, there is increased recognition that it may not be sufficient to fully address the uncertainty and complexity inherent at the telecommunications sector or system level.

TPDC definition of sector resilience

Sector resilience is the ability of a *sector* to sustain performance of critical services to end-users and across the nation in the face of unspecific, and possibly unforeseen, disruptive events. Building sector resilience requires a clearly articulated **shared vision** across the vast range of stakeholders that make up the sector. Sector resilience is enabled by the **capacity** to manage the phases of disruption: to prepare, absorb, adapt, respond, recover, learn and transform from disruptions in a timely and efficient manner.¹²

Resilience depends on developing sophisticated and dynamic **disruption management approaches**:

- risk management: including situational awareness of the risk landscape to inform action at all phases of disruption
- consequence management: to minimise impact and offset the harm of disruptive events when they occur
- lessons management: to learn from past disruptions and embed lessons to mature sector capacities and capabilities.

TPDC definition of systemic resilience

Systemic resilience of all national critical infrastructure depends on sector-level resilience. It arises dynamically when all sectors of critical national infrastructure can provide agreed critical services, despite internal or external disruption.¹³

The goal of systemic resilience should reflect the nation’s ambitions for uninterrupted critical services (i.e. a shared vision).¹⁴

10 Risk and Resilience Expert Panelist, 2024.

11 International Organization for Standardization 2021, *ISO 31000 — Risk Management*, <https://www.iso.org/iso-31000-risk-management.html/>

12 Organisation for Economic Development n.d., *Guidelines for Resilience Systems Analysis: How to Analyse Risk and Build a Roadmap to Resilience*, OECD iLibrary, https://www.oecd-ilibrary.org/development/guidelines-for-resilience-systems-analysis-how-to-analyse-risk-and-build-a-roadmap-to-resilience_3b1d3efe-en

13 United Nations Office for Disaster Risk Reduction, “Principles for Resilient Infrastructure,” 2021, <https://www.undrr.org/publication/principles-resilient-infrastructure>.

14 Organisation for Economic Development n.d., *Guidelines for Resilience Systems Analysis: How to Analyse Risk and Build a Roadmap to Resilience*, OECD iLibrary, https://www.oecd-ilibrary.org/development/guidelines-for-resilience-systems-analysis-how-to-analyse-risk-and-build-a-roadmap-to-resilience_3b1d3efe-en

A shared vision and language of sector resilience

Australia does not currently have a shared vision for sector-wide telecommunications resilience.

Resilience is an elusive concept that requires collective action and, therefore, a shared vision. Such a shared vision guides individual lines of effort, aids prioritisation, and justifies the resourcing needed to sustain performance across the vast range of stakeholders that make up the telecommunications sector.¹⁵

A shared vision allows stakeholders to recognise their interdependencies and work together with a common understanding of the sector's purpose and challenges.¹⁶

This Profile, and especially the Sector Resilience Maturity Model and Assessment herein, provides the foundation for such a shared vision and a common lexicon for stakeholders.

Resilience is enabled by capacity to manage across the phases of disruption

In this Profile, 'phases of disruption management' refers to the different capacities that are needed to deal with disruption divided into three disruption management approaches:

- risk management
- consequence management
- lessons management.

Phases of disruption management are not discrete and linear but dynamic, overlapping and repeating.

A sector is resilient when it has matured the capacities required to sustain performance with a high degree of reliability in the face of disruption. These capacities must be built across all phases of disruption management: to prepare, absorb, adapt, respond, recover, learn and transform from disruptions in a timely and efficient manner.¹⁷

Building these capacities is part of a comprehensive strategy for managing every phase of disruption and, therefore, building resilience. It's not just about reacting when problems happen, but also about preparing before they occur, responding during, and learning afterwards.

The sections below outline key resilience capacities at the sector-level, each mapped to a phase of disruption management. Each phase is discussed in turn below and is crucial for building a resilient telecommunications sector capable of withstanding and evolving in the face of various challenges.

¹⁵ See Part 2, Step 1: Defining the Sector.

¹⁶ Department of Home Affairs 2023, 2023–2030 Australian Cyber Security Strategy, <https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf>

¹⁷ Connelly, E, Allen, C, Hatfield, K, Palma-Oliveira, J, Woods, D & Linkov, I 2017, *Features of Resilience*, Environment Systems & Decisions, <https://doi.org/10.1007/s10669-017-9634-9>

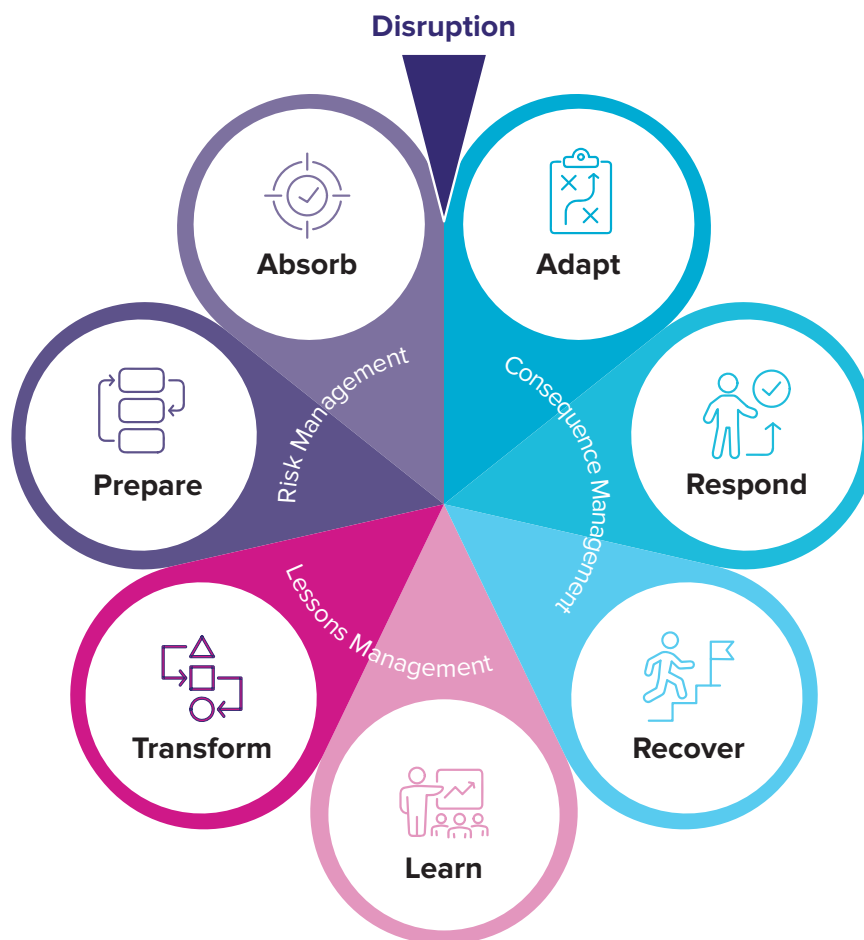
Table 1. Understanding resilience capacities across all phases of disruption management¹⁸

Resilience capacity (Phases of disruption management)	TPDC definition	Disruption management approaches
Prepare	Preparedness capacity in the context of telecommunications resilience refers to the sector's ability to mitigate and prepare for disruption. This capacity is sustained by having situational awareness of the risk horizon and then implementing mitigation and planning capabilities to ensure that critical assets and services can withstand, absorb, and recover from disruption. It includes the governance processes that enable the sector to adapt, respond to, learn from, and transform after disruptive events.	Risk management
Absorb	Absorptive capacity in the context of telecommunications resilience refers to the sector's ability to cope with disruption. This capacity is sustained by the robustness of technical infrastructure and coping strategies that enhance the sector's ability to absorb shocks without significant service degradation or failure.	
Adapt	Adaptive capacity in the context of telecommunications resilience refers to the sector's ability to prepare for disruption in advance and make positive adjustments that counter the impacts of disruption. This capacity is sustained by situational awareness of the risk horizon, flexible and responsive operational capabilities, continuous monitoring, and the ability to modify systems and processes in response to emerging threats and changes.	Consequence management
Respond	Responsive capacity in the context of telecommunications resilience refers to the sector's ability to quickly and effectively respond to disruptions. This capacity is sustained by building consequence management capabilities, including establishing incident response protocols, real-time communication systems, and coordinated efforts among stakeholders to manage and mitigate the impacts of disruptions.	
Recover	Recovery capacity in the context of telecommunications resilience refers to the sector's ability to restore services and return to normal operations following a disruption. This capacity is sustained by building consequence management capabilities, including comprehensive recovery planning, resource allocation, and support systems that enable rapid restoration of critical functions. It also includes strategies to support long-term community recovery, ensuring that telecommunications services contribute to affected communities' overall resilience and well-being.	

¹⁸ In this profile, 'phases of disruption management' refers to the different capacities that are needed to deal with disruption. These are not discrete and linear 'stages' but are phases that overlap.

Resilience capacity (Phases of disruption management)	TPDC definition	Disruption management approaches
Learn	Learning capacity in the context of telecommunications resilience refers to the sector's ability to learn from past disruptions and continuously improve its resilience strategies. This capacity is sustained by systematically analysing disruptions, feedback mechanisms, and integrating lessons learned into planning and operations.	Lessons management
Transform	Transformative capacity in the context of telecommunications resilience refers to the sector's ability to fundamentally change and improve its systems and processes in response to evolving threats, threat sources, and vulnerabilities. This capacity is sustained by innovation, forward-thinking governance, and the ability to implement strategic changes that enhance overall resilience.	

Figure 2. Resilience capacities can be built over all phases of the disruption management process for continuous learning and improvement



Risk management

In the context of sector-level resilience, risk management is the process of developing situational awareness of the factors of risk (threats, threat sources, vulnerabilities) and anticipating their potential consequences.¹⁹

Situational awareness equips decision-makers and policymakers with the necessary information to make informed decisions about the telecommunications sector, its entities, stakeholders, assets, and services.²⁰

Risk isn't a static picture; it is dynamic.²¹ Resilience is also an emergent property; therefore, this Profile refers throughout to the risk horizon rather than a risk landscape.²²

Risk emerges from dynamic interactions between a range of factors that cause disruption: non-malicious and malicious threat sources, threats and vulnerabilities. These interact to cause consequences that are unpredictable in magnitude and impact.

In this Profile, risk management is a disruption management approach that has been used to frame evidence and then identify potential capabilities that can be enhanced or matured through the Resilience Maturity Model.

Step 2 of this Profile includes a compilation of evidence regarding the risk factors (threat sources, threats and vulnerabilities).

Box 1. Example of how the factors of risk can lead to a disruptive event in the Australian telecommunications sector

An arsonist (a malicious threat source) or bolt of lightning (an unmalicious threat source) may cause a bushfire (a threat) in a field.

The field contains an above-ground telecommunications asset. The asset is surrounded by long, dry grass that has been caused by a lack of maintenance (a vulnerability). In this instance, the threat (bushfire) may manifest as a disruptive event and damage the asset.

If the asset is damaged (a disruptive event), this may prevent a major telecommunications provider (an entity) from providing uninterrupted services (consequence) to a town for a number of hours (the magnitude of consequence).

19 International Standards Organization, December 7, 2021, *ISO 31000 — Risk Management*, <https://www.iso.org/iso-31000-risk-management.html/>

20 Conges, A, Breard, L, Patruno, W, Ouro-Sao, A, Salatge, N, Fertier, A, Lauras, M, Graham, J, Benaben, F 2023, 'Situational Awareness and Decision-making in a Crisis Situation: A Crisis Management Cell in Virtual Reality', *International Journal of Disaster Risk Reduction*, vol. 97, <https://doi.org/10.1016/j.ijdrr.2023.104002>

21 Darnhofer, I 2021, *Farming Resilience: From Maintaining States Towards Shaping Transformative Change Processes*, Department of Economics and Social Sciences Austria, <https://doi.org/10.3390/su13063387>

22 Kaloudi, N & Li, J 2021, *Comparison of Risk Analysis Approaches for Analyzing Emergent Misbehavior in Autonomous Systems*, Department of Computer Science, Norwegian University of Science and Technology, <https://www.rpsonline.com.sg/proceedings/9789811820168/pdf/213.pdf>

Consequence management

Consequence management is the operational approach to lessening the impact and offsetting the harm during and after disruptions to all who feel them.²³

At the sector-level, national consequence management requires maturing capacities and building capabilities within the enabling environment through regulation, coordination, cooperation and collective action.

The telecommunications sector has a vast range of stakeholders that need to be integrated, steered, stimulated, and incentivised to cooperate and innovate. Without a clear delineation of roles or incentives for action, organisations may choose to prioritise their own interests when disruption occurs, resulting in suboptimal outcomes for the entire sector.

In this Profile, consequence management is a disruption management approach that has been used to frame evidence and then identify potential capabilities that can be enhanced and matured through the Sector Resilience Maturity Model.

Step 2 of this Profile contains a compilation of evidence detailing the state of consequence management in the Australian telecommunications sector.

Box 2. Disturbance vs. disruption

In the telecommunications sector, threats and vulnerabilities can exist without rising to the level of disruption. Instead, they may result in disturbances such as service slowdowns or temporary interruptions.

While disturbances do not severely compromise performance, they necessitate ongoing monitoring and management. Disturbances can typically be addressed by individual enterprises using standard operational procedures without necessitating extraordinary measures. They are regarded as expected occurrences within normal business operations, exerting minimal impact on end-users and posing a minimal threat to the safety or lives of the Australian public.

In contrast, a disruption is characterised by:

- consequences that have escalated to a point where they have ‘run-away’; they cannot be easily contained or reversed
- technical, non-technical, and social systems and resources are overwhelmed
- governance structures and strategic and operational decision-making functions are degraded or disabled
- consequences span multiple jurisdictions and have cross-sectoral effects, including social and economic effects on a range of end-users
- consequences are cascading, compounding, interacting, and interconnecting
- consequences are perceived as more than an inconvenience and potentially catastrophic by relevant stakeholders or end-users.

The line between an inconvenient disturbance and a catastrophic disruption is not strictly binary. The magnitude of consequences can escalate quickly from manageable to critical. Decision points are complex and nuanced. The spectrum of normal operational capacity can rapidly be exceeded, leading to overwhelmed systems. Effective consequence management requires recognising this spectrum and responding appropriately as situations evolve.

²³ Emergency Management Victoria 2022, *Consequence Management*, <https://www.emv.vic.gov.au/responsibilities/consequence-management>

Lessons management

Lessons management is an integrated principled approach to capturing, analysing and applying lessons learned from past experiences to transform and improve future performance.²⁴

Transformation involves creating deliberate, profound change by altering a system's underlying patterns and structures, either partially or wholly. This change fosters new patterns of thinking and practice, which coalesce over time into new approaches.²⁵ Effective transformation relies on good lessons management, where lessons are identified and enacted within organisations by decision-makers, and in government by policymakers.

Lessons management takes a principled approach to maturing resilience capacities and building capabilities across the phases of disruption management.²⁶ Resilience is not a static characteristic, but rather a continuous, iterative process of learning and transformation.²⁷

Adopting a principled approach to lessons management improves the sector's capacity to manage the consequences of disruptions when they occur.

In turn, mature lessons management and consequence management sharpen the sector's capacity to manage the dynamic risk horizon.

An integral part of lessons management is change management.²⁸ The sector's ability to integrate change is limited unless the change can be observed across the sector, and it can be determined that the lessons were learned sector-wide – that is, the actions taken have improved sectoral resilience.

In this Profile, lessons management is a disruption management approach that has been used to synthesise and structure evidence gathered about risk and consequence management to identify capabilities that can be enhanced or matured in the Sector Maturity Model.

Together, this integrated approach to managing disruptions (encompassing risk management, consequence management and lessons management) provides the framework to assess and mature sector resilience.

The Sector Resilience Maturity Model and Assessment in Part 1 of this Profile evaluates resilience maturity across the Australian telecommunications sector.

24 Crawley, H, Eburn, M, Logan, K, Beekhar, D, Strickland, R, Thomason, M & Males, J 2019, *Lessons Management Handbook*, Australian Institute for Disaster Resilience, https://www.aidr.org.au/media/1760/aidr_handbookcollection_lessonsmanagement_2019.pdf

25 Australian Resilience Centre 2021, *Transforming Systems*, <https://www.ausresilience.com.au/transforming-systems>

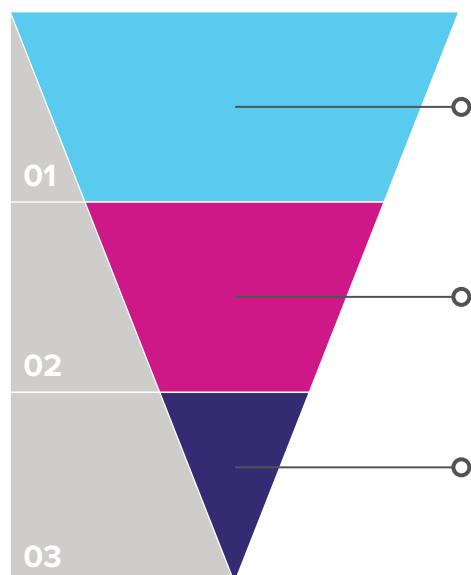
26 Crawley, H, Eburn, M, Logan, K, Beekhar, D, Strickland, R, Thomason, M & Males, J 2019, *Lessons Management Handbook*, Australian Institute for Disaster Resilience, https://www.aidr.org.au/media/1760/aidr_handbookcollection_lessonsmanagement_2019.pdf

27 Mentges, A, Halekotte, L, Schneider, M, Demmer T & Lichte, D 2023, 'A Resilience Glossary Shaped by Context: Reviewing Resilience-related Terms for Critical Infrastructures', *International Journal of Disaster Risk Reduction*, vol. 96, <https://doi.org/10.1016/j.ijdr.2023.103893>

28 Crawley, H, Eburn, M, Logan, K, Beekhar, D, Strickland, R, Thomason, M & Males, J 2019, *Lessons Management Handbook*, Australian Institute for Disaster Resilience, https://www.aidr.org.au/media/1760/aidr_handbookcollection_lessonsmanagement_2019.pdf

Systemic resilience

Maturing sector resilience in the telecommunications sector (that is, risk management, consequence management, and lessons management) will contribute to the development of systemic resilience across all critical infrastructure, while also enhancing enterprise resilience.²⁹



At the systemic-level, the goal is to ensure that the performance of telecommunications services is reliably sustained and available to other critical infrastructure sectors, and vice versa (given mutual interdependencies). This level of ambition should match what the country wants and needs in terms of uninterrupted essential services.³⁰

At the sector-level, it's important to think of telecommunications as a broad sector, not just individual operators. Everyone involved – phone and internet providers, government regulators, and other essential services that rely on telecommunications, and the communities that rely on them – all share a responsibility. This shared responsibility is the foundation for building resilience to ensure that people can still communicate when necessary, even in the face of disruption. This is the level of resilience assessed in the Profile.

At the enterprise-level, resilience should not be perceived as reaching a final endpoint but as building up many capacities that can, as necessary, be scaffolded-down and scaled-up. Enterprise resilience involves nuanced interactions between technical, organisational, economic, and social capabilities that combine to maintain performance in the face of disruption.

Operationalising the approach to resilience articulated in this Profile will strengthen system, sector, and enterprise resilience by stimulating and incentivising cooperation, innovation, and continuous improvement by all stakeholders.

²⁹ Ungar, M 2018, 'Systemic Resilience: Principles and Processes for a Science of Change in Contexts of Adversity Principles and Processes for a Science of Change in Contexts of Adversity', Ecology and Society vol. 23, <https://www.jstor.org/stable/26796886>

³⁰ Organisation for Economic Development n.d., *Guidelines for Resilience Systems Analysis: How to Analyse Risk and Build a Roadmap to Resilience*, OECD iLibrary, https://www.oecd-ilibrary.org/development/guidelines-for-resilience-systems-analysis-how-to-analyse-risk-and-build-a-roadmap-to-resilience_3b1d3efe-en

The Sector Resilience Maturity Model

Until now, there has been no comprehensive framework to evaluate sector-level resilience. To fill this gap, TPDC developed the Sector Resilience Maturity Model (SRMM).

Resilience in the telecommunications sector is enabled by the development of a shared vision. In this report, we present a shared vision of resilience in the Australian telecommunications sector. This vision takes the form of an SRMM, which outlines the Principles, Capabilities and Resources needed to mature the sector in the face of uncertainty.

The vision present in the SRMM is a synthesis of evidence gathered between February 2023 and May 2024 across a multi-stage research and engagement process, with the participation of 204 stakeholders and endorsed by the 26-member Expert panel.

The SRMM emphasises the need to mature dynamic capabilities across risk management, consequence management, and lessons management to manage the phases of disruption in a timely and efficient manner, while preparing for an unknown future.

The SRMM provides a holistic and integrated approach to mature the resilience of the whole sector by defining the Principles, Capabilities and Resources needed at the sector-level (see Figure 2). Over time, these should be evaluated to continuously improve efforts, sharpen collaboration, shared goals, and align incentives.

TPDC Sector Resilience Maturity Model

The **TPDC Sector Resilience Maturity Model (SRMM)** is a model developed specifically to evaluate sector-level resilience.

The Model is structured around **three key components**, critical in measuring and maturing a sector's approach to building and sustaining resilience:

- **Resilience principles:** the foundational vision steering resilience efforts
- **Resilience capabilities:** the specific actions that enable the sector to manage disruptions
- **Resilience resources:** the necessary assets to support these efforts.

To produce a maturity assessment, each component of the SRRM is evaluated across a sequence of **five maturity levels** that lead to systemic transformations:

1. **Initial:** Resilience practices are unstructured and reactive across the sector
2. **Developing:** Basic resilience measures are in place, including initial sectoral coordination efforts
3. **Defined:** Resilience processes are well-defined and documented across the sector
4. **Managed:** Resilience practices are systematically integrated and consistently applied across the sector
5. **Optimised:** Resilience is continuously improved through proactive learning, innovation and transformation.

The RMM establishes a **common understanding** of resilience maturity and how to achieve it. It aids decision-makers and policymakers in developing a **shared vision** for maturing sectoral resilience.

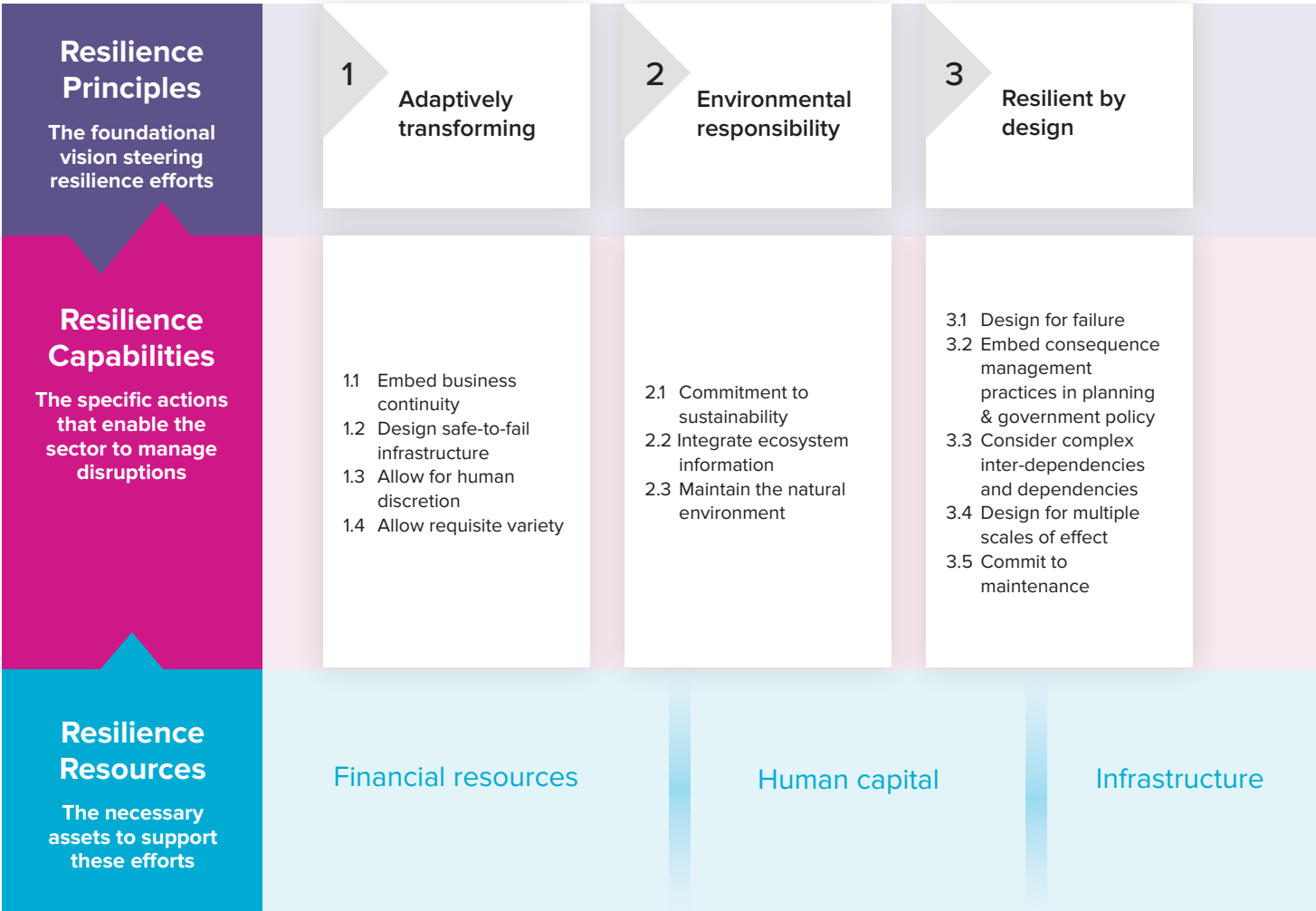
Applying evidence to the RMM produces a **point-in-time maturity assessment** of resilience. Such an assessment should be conducted regularly (annually or biannually) to assess progress.

The RMM is a **sector-level assessment** that can foster synergies in the collective efforts of all sector stakeholders. For example, this Model could also serve as a **self-assessment tool for individual enterprises** of their maturity level, with reference to sector outcomes.

While TPDC developed the SRMM to assess resilience in the telecommunications sector, the Model could equally be applied to assess the resilience maturity of other critical infrastructure sectors in Australia, or internationally.

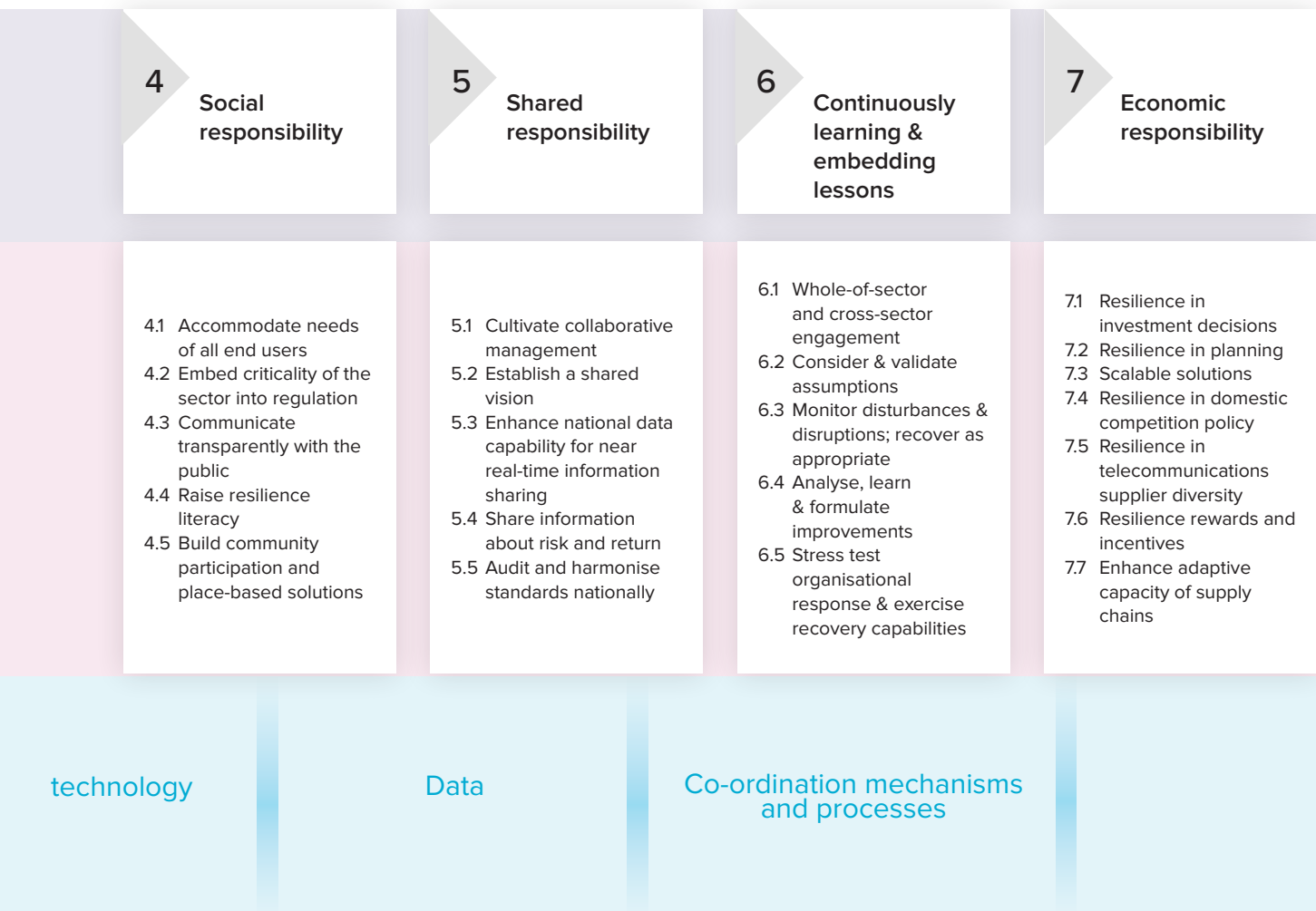
Figure 3. Overview of the Sector Resilience Maturity Model

Assess the sector against resilience principles, capabilities & resources



Assess the maturity of each factor on a scale of 1 to 5





Assessment of telecommunications sector resilience maturity

After developing the SRRM, TPDC applied the evidence collected throughout the life of this project to the Model, to inform the following assessment of the telecommunications sector's resilience maturity. This assessment creates a benchmark against which progress can be monitored on an ongoing basis.

This assessment represents a whole-of-sector systems view of the resilience maturity of the whole telecommunications sector, not individual enterprises.

The sector includes local, state/territory, and federal governments and stakeholders who provide telecommunications services and assets that contribute to the connectivity and overarching purpose of the sector. It encompasses their supply chains, consumers, regulators, end-users, developers, suppliers, and others who are influenced by the sector (see *Defining the Sector*).

This assessment should not be construed as a criticism of the sector's ability to respond to business-as-usual *disturbances* to deliver its core functions effectively. Rather, it points to the need to sharpen approaches to *disruption*. These include more effective deployment of resources across phases of disruption management, and between the vast range of stakeholders that define the sector.

The assessment of Australia's telecommunications sector did not seek to evaluate individual enterprises in the telecommunications industry, nor did it seek to evaluate its ability to respond to business-as-usual disturbances in performance to deliver core functions effectively.³¹

Many individual enterprises have long-established resilience frameworks, design principles, and risk management processes to serve these purposes, such as problem and incident management systems, and crisis management protocols. These are in place at individual enterprises such as service providers, some local and state/territory governments, and a few federal agencies.

Where industry self-assesses that its resilience maturity is ahead of other stakeholders in the sector, then this is an opportunity for those enterprises to share lessons learned and guide whole-of-sector improvement.

³¹ See Box 2 – Disturbance vs Disruption (page 15).

Overall, the TPDC and the project's Expert Panel assess that the Australian telecommunications sector is currently at the 'Developing (level 2)' of resilience maturity.

The assessment is based on evidence collected over 2023-2024. It creates a benchmark against which progress can be monitored on an ongoing basis.

Assessments of the sector's maturity against a range of factors, including resilience principles, capabilities, and resourcing, contribute to this overall maturity score.

Principles: the sector is developing (level 2). Seven principles have been identified to guide and align resilience efforts. These encompass adaptive transformation, environmental responsibility, resilience by design, social responsibility, shared responsibility, continuous learning and embedding lessons, and economic responsibility. Most were assessed to be developing (2), with one principle – shared responsibility – determined to be the lowest, with a score of initial (1). This indicates that individual organisations are guided by social, economic, and environmental resilience principles, but these efforts are fragmented and not cohesively aligned across the sector.

Capabilities: the sector is developing (level 2). Thirty-four capabilities have been identified that serve as goals for the sector. These include specific actions that can better enable the sector to manage risk and the consequences of disruption. Across 34 capabilities, the sector was found to be more mature (level 3) when it comes to asset maintenance and infrastructure hardening. It was significantly less mature (level 1) for other resilience capabilities, such as those relating to data, standardisation, cross-sector engagement, and consequence management.

Resourcing: the sector is developing (level 2). Resources encompass financial, human capital, infrastructure and technology, data, and coordination mechanisms and processes. Across five major resource categories, some resources, such as physical assets and technological solutions, are dedicated to resilience and were found to have a higher level of maturity (level 3). However, significant gaps remain for resources to support data gathering, which informs real-time situational awareness, and for investment in resilience initiatives and emergency funds to assist with responses to unexpected disruptions (level 1).

The assessment shows that in some areas, the sector has a sector maturity score higher (level 3) than the overall assessment (level 2) in areas like environmental sustainability, infrastructure maintenance and hardening, and raising resilience literacy. However, as a whole, it lacks standardisation, integration, and continuous improvement mechanisms for resilience (areas determined to be at level 1).





One area that needs immediate attention to improve resilience is shared responsibility (resilience principle 3). The assessment showed there are currently deficiencies across a range of capabilities linked to shared responsibility. These include consequence management, establishing a shared vision, enhancing national data capabilities for information sharing, harmonising standards, and fostering cross-sector engagement.

The lack of shared responsibility leads to fractured efforts and a lack of coherence sector-wide, particularly in responding to complex disruptions that require coordinated action across multiple stakeholders. Our consultations showed that resilience is sometimes treated as someone else's problem, so it ends up being nobody's responsibility.

Resilience principles

Resilience Principles serve as foundational pillars to guide the sector's resilience efforts.³² It is important to consider that each principle is formulated on a sector-wide basis, emphasising and prioritising the whole-of-sector resilience capability. Table 2 describes each principle and provides an assessment of the Australian Telecommunications sector's current maturity against each principle.³³




Table 2. Assessment of Australian telecommunications sector maturity against the Resilience Principles

Resilience Principle	Description Of The Principle	Current Sector Maturity Level
1. Adaptively transforming	<p>We often assume the future will mirror the past, and Australia's telecommunications sector demands will evolve over time. To address this, our systems must be designed with flexibility in mind, ensuring that supply chains, organisational structures, and operational processes can adapt to new and unforeseen challenges.</p> <p>The Australian telecommunications sector must be ready for unexpected disruptions, including cyber threats, natural disasters, and rapid technological changes. Embracing complexity is crucial for creating adaptive telecommunications infrastructure. By consistently updating infrastructure, management, and information systems based on new insights, the sector can remain robust and responsive.</p> <p>A resilient telecommunications sector must be able to adapt and transform rather than just bounce back.³⁴</p>	<p>Developing (2)</p> 
2. Environmental responsibility	<p>This principle acknowledges the significance of minimising harm to the natural environment, such as by reducing the sector's ecological footprint, while also exploring opportunities to positively interact with the environment to enhance and mitigate climate and environmental threats and vulnerabilities.</p>	<p>Developing (2)</p> 
3. Resilient by design	<p>This principle acknowledges that investing in readiness for disruption is most effective during the design phase, where there is an opportunity to consider the potential impacts from disruptive events. This involves evaluating how such events could affect the entire lifecycle of infrastructure provision. While some systems within the sector (i.e. network architecture) may be more mature, this principle pertains to the sector as a whole, including dependencies and interdependencies, processes, and coordination mechanisms.</p>	<p>Developing (2)</p> 
4. Social Responsibility	<p>The Australian telecommunications sector is a complex socio-technical system – made up of tightly coupled engineered and technical assets that are embedded in society and linked with economies and the public through the provision of services. Therefore, as a provider of a public service, the telecommunications sector bears a social responsibility to Australians.</p>	<p>Developing (2)</p> 

³² Adapted from United Nations Office for Disaster Risk Reduction 2021, *Principles for Resilient Infrastructure*, <https://www.undrr.org/publication/principles-resilient-infrastructure>

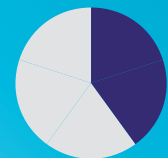
³³ Assessment ratings were made by averaging the ratings given for capabilities and resources. Each assessment maturity level has been informed by evidence collected over the life of this project (see *Part 2 – Evidence in Support of Assessment*).

³⁴ Singh, P, Amekudzi-Kennedy, A, Ashuri, B, Chester, M, Labi, S & Wall, T 2022, *Developing Adaptive Resilience in Infrastructure Systems: An Approach to Quantify Long-term Benefits*, Sustainable and Resilient Infrastructure 8, <https://doi.org/10.1080/23789689.2022.2126631>

Resilience Principle	Description Of The Principle	Current Sector Maturity Level
5. Shared Responsibility	Resilience is not solely an individual effort but rather a shared responsibility, requiring collaboration among stakeholders and a shared vision. ³⁵ This collaborative effort seeks to foster cohesion between commercial imperatives and sector-level outcomes, ensuring service continuity by incentivising collective action and mutual support. This principle acknowledges that entities within the Australian telecommunications sector should foster collaboration to share data, knowledge, and expertise. Standardised data exchange enables insights into the risk horizon, while international and cross-sectoral efforts are crucial to prevent cascading failures due to complex interdependencies across sectors and geographies. ³⁶	Initial (1) 
6. Continuously learning and embedding lessons	Continuously learning and embedding lessons in the Australian telecommunications sector is crucial, due to the internal complexity and external hyperconnectivity of its infrastructure. ³⁷	Developing (2) 
7. Economic responsibility	<p>Resilience in economic decision-making requires a paradigm shift. Resilience in planning involves ensuring that investments in infrastructure and technology are both cost-effective and sustainable over the long term. This principle encourages the strategic allocation of resources to enhance the robustness and adaptability of telecom networks against disruptions, such as natural disasters or cyber-attacks, while also considering the financial impact on stakeholders and consumers.</p> <p>Competition policy can be refined to remove barriers to cooperation on resilience-enhancing activities, and includes building adaptive approaches to operational continuity and sustainability. The intention is to minimise potential economic losses during unforeseen events, but also to promote trust and reliability, ensure diverse supply, and allow investment decisions to enhance the ability to respond and recover. The development of incentives and rewards will maintain customer satisfaction, and operational stability, and make resilience a commercial differentiator.</p>	Developing (2) 



Overall assessment of the Australian telecommunications sector maturity against the TPDC Resilience Principles



**Developing
2**

35 Organisation for Economic Development n.d., *Guidelines for Resilience Systems Analysis: How to Analyse Risk and Build a Roadmap to Resilience*, OECD iLibrary, https://www.oecd-ilibrary.org/development/guidelines-for-resilience-systems-analysis-how-to-analyse-risk-and-build-a-roadmap-to-resilience_3b1d3efe-en

36 Pescaroli, G & Alexander, D 2018, 'Understanding Compound, Interconnected, Interacting, and Cascading Risks: A Holistic Framework', *Risk Analysis* vol. 38, <https://doi.org/10.1111/risa.13128>



37 Crawley, H, Eburn, M, Logan, K, Beekhar, D, Strickland, R, Thomason, M & Males, J 2019, *Lessons Management Handbook*, Australian Institute for Disaster Resilience, https://www.aidr.org.au/media/1760/aidr_handbookcollection_lessonsmanagement_2019.pdf

Resilience capabilities

The Resilience Capabilities serve as goals for the sector to strive for in strengthening its resilience capacities.³⁸ They include specific actions that can better enable the sector to manage risk and the consequences of disruption.

Table 3 describes each capability and is organised by their associated Resilience Principles.³⁹

Table 3. Assessment of Australian telecommunications sector maturity against the TPDC Resilience Capabilities

Resilience Capabilities	Description of the Capability	Opportunity to Improve Sector Resilience	Current Sector Maturity Level
1. Adaptively transforming			
1.1 Embed business continuity management and anticipated improvisation	Organisational resilience in the Australian telecommunications sector hinges on two complementary strategies: business continuity management for predictable disruptions, and the need to ‘anticipate improvisation’ for unforeseen, high-impact events. ⁴⁰	These strategies build sectoral resilience and can be expanded nationally through comprehensive national continuity planning ⁴¹ and large-scale anticipated improvisation playbooks. At the enterprise-level, approaches are aligned and coherent with broader systemic resilience.	<p>Developing (2)</p> 
1.2 Design safe-to-fail infrastructure	Potential failures are explicitly considered from an all-hazards perspective during the development process. While traditional infrastructure design focuses on optimising functional capacity by balancing cost and performance, it often assumes that failures can be prevented with adequate safety margins. However, embracing the concept of safe-to-fail infrastructure is essential.	Designing systems that acknowledge the possibility of failure, but ensure that when failures occur, they do so in a manner that does not compromise safety. ⁴²	<p>Defined (3)</p> 





38 United Nations Office for Disaster Risk Reduction 2021, *Principles for Resilient Infrastructure*, <https://www.undrr.org/publication/principles-resilient-infrastructure>

39 The assessment is informed by evidence collected over the life of this project (compiled at *Part 2 – Evidence in Support of Assessment* below), and provides an assessment of the Australian Telecommunications Sector’s current maturity against each principle.

40 Steen, R, Haug, O & Patriarca R, 2023, ‘Business Continuity and Resilience Management: A Conceptual Framework’, *Journal of Contingencies and Crisis Management*, vol. 32, <https://doi.org/10.1111/1468-5973.12501>

41 Barnes, P & Bergin, A 2020, *Risk, Resilience & Crisis Preparedness, After COVID 19: Australia and the World Rebuild*, Australian Strategic Policy Institute, https://www.academia.edu/43153398/Risk_Resilience_and_Crisis_Preparedness

42 Chester, M, Underwood, B, Allenby, B, Garcia, M, Samaras, C, Markolf, S, Sanders, K, Preston, B & Miller, T 2021, ‘Infrastructure Resilience to Navigate Increasingly Uncertain and Complex Conditions in the Anthropocene’, *Npj Urban Sustainability*, vol. 1, no. 1, <https://doi.org/10.1038/s42949-021-00016-y>




Resilience Capabilities	Description of the Capability	Opportunity to Improve Sector Resilience	Current Sector Maturity Level
1.3 Allow for human discretion	Commercial pressures and technological advancements are driving workforce reductions and increasing automation to remain competitive. ⁴³ This trend has led to the development of highly integrated infrastructure to improve cost efficiency.	Safeguarding manual overrides and human-in-the-loop provisions maintain human discretion in critical decision-making processes, such as network troubleshooting and patching, or customer service.	Defined (3) 
1.4 Adopt approaches to defining requisite variety⁴⁴	Organisational structures, processes, and systems are diverse, flexible, and extensible. The same principle applies to diversification of supply chains, skills, and technical components of networks.	Ensuring variety enhances the sector's ability to absorb, adapt, respond, and recover effectively.	Initial (1) ⁴⁵ 
2. Environmental responsibility			
2.1 Commitment to sustainability	Infrastructure systems can directly contribute to disasters with an environmental threat vector or induce long-term negative impacts on their surrounding environments.	Prioritising sustainability initiatives is essential for the sector to mitigate environmental risk and promote environmental resilience. By moving towards a circular economy and actively reducing emissions, the sector can lessen the risk of triggering disasters with an environmental threat vector. ⁴⁶	Developing (2) 
2.2 Integrate ecosystem information	Data on climate futures is integrated into decision-making processes.	By leveraging ecosystem information, the sector can better anticipate and mitigate environmental impacts. This proactive approach minimises not only ecological harm, but also fosters long-term environmental stewardship, bolstering the sector's ability to adapt and thrive in a changing climate.	Developing (2) 




⁴³ Attaran, M 2021, *The Impact of 5G on the Evolution of Intelligent Automation and Industry Digitization*, *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 5, <https://doi.org/10.1007/s12652-020-02521-x>

⁴⁴ Heylighen, F & Joslyn, C 2003, *Cybernetics and Second-Order Cybernetics*, Elsevier eBooks, <https://doi.org/10.1016/b0-12-227240-4/00178-7>




⁴⁵ Note: TPDC assess the maturity of supply chain diversification in isolation to be at the 'defined (3)' level.





⁴⁶ Hailemariam, A & Erdiaw-Kwasie, M 2022, *Towards a Circular Economy: Implications for Emission Reduction and Environmental Sustainability*, *Business Strategy and the Environment*, vol. 32, <https://doi.org/10.1002/bse.3229>





Resilience Capabilities	Description of the Capability	Opportunity to Improve Sector Resilience	Current Sector Maturity Level
2.3 Maintain the natural environment	Proactively managing the natural environment around infrastructure locations reduces vulnerabilities and the chance of environment-driven disruption.	Management approaches may include, but are not limited to, reducing overgrown vegetation, erosion control measures, and deploying innovative technologies like smart sensors and predictive analytics to enhance real-time monitoring of environmental conditions.	Defined (3) 
3. Resilient by design			
3.1 Design for failure	<p>Failures are inevitable. Intentionally planning for and accommodating potential system failures or disruptions during the design and implementation phases of telecommunications assets and services minimises the impact of failure on service delivery and overall system functionality.</p> <p>Strategies for designing for failure may include monitoring measures, robust backup systems, such as limited purpose networks, network segmentation (either geographic, application or service-specific), and contingency plans to ensure continuity of operations in the event of outages or failures.</p>	Building systems with multiple means of interconnection and enable rapid failover utilising independent platforms, such as internet exchange points, should be encouraged. The goal is to build resilient infrastructure to withstand various challenges and maintain essential services, even under adverse conditions.	Developing (2) 
3.2 Embed consequence management practices in enterprise planning and government policy	Consequence management practices (including, but not limited to, business continuity plans, recovery and reactivation of service capability and anticipated improvisation practices) are embedded from the outset of infrastructure or service design.	By integrating these practices early on, all stakeholders across the sector can proactively anticipate and prepare for potential disruptions, ensuring that they have the necessary strategies and resources in place to effectively manage and mitigate a range of anticipated and unanticipated consequences.	Initial (1) 




Resilience Capabilities	Description of the Capability	Opportunity to Improve Sector Resilience	Current Sector Maturity Level
3.3 Consider complex interdependencies and dependencies	Mapping and understanding the intricate connections and dependencies that exist within and across critical infrastructure systems, including technological, organisational, social and environmental factors, can help identify vulnerabilities and points at which consequences may cascade or compound.	Entities can identify points to focus on activities that prepare the sector for disruptions and how to limit a cascade or escalation of the impact.	Developing (2) 
3.4 Design for multiple scales of effect	To maximise the efficacy of resilience investments, solutions are designed to account for multiple scales of disruption impact.	Designs may include implementing preventative and adaptive measures to enhance resilience across various disaster scales, geopolitical contexts (encompassing individual infrastructures, communities, cities, and broader regional and national levels), and different timeframes (ranging from immediate to long-term). ⁴⁷	Initial (1) 
3.5 Commit to maintenance	Comprehensive infrastructure asset management schemes are established from the outset of asset design. This includes maintaining an inventory of all assets and their operational conditions, and managing strategic, financial, and technical aspects throughout their lifecycle.	Integrating routine maintenance, such as yearly inspections, with periodic maintenance can extend the lifespan of infrastructure and improve performance levels over time. For example, by regularly inspecting network equipment and implementing timely repairs or upgrades, telecommunications enterprises can ensure optimal functionality and longevity of their infrastructure assets, thereby enhancing service reliability and customer satisfaction.	Defined (3) 




⁴⁷ Naheed, S 2021, *Understanding Disaster Risk Reduction and Resilience: A Conceptual Framework*, Springer eBooks, https://doi.org/10.1007/978-3-030-61278-8_1




Resilience Capabilities	Description of the Capability	Opportunity to Improve Sector Resilience	Current Sector Maturity Level
4. Social responsibility			
4.1 Understand and accommodate the needs of all end-users	The needs of all end-users, including marginalised groups such as those living with disabilities, remote residents, and Aboriginal or Torres Strait Islander communities, are understood and prioritised.	By centring their needs in the design and delivery of telecommunications services, entities can promote inclusivity and accessibility. This may include implementing measures such as providing alternative communication options, improving coverage in remote areas, and offering culturally sensitive services.	Developing (2) 
4.2 Embed the criticality of telecommunications into regulation	Telecommunications is both a social and economic enabler, and a public good. It plays a crucial role in supporting emergency services, enabling the digital economy, and ensuring the enforceability of the supply of essential services across the entire economy and society. From facilitating rapid response during crises to powering e-commerce and digital innovation, telecommunications underpins the functioning of modern life.	Acknowledging telecommunications as the cornerstone of interdependent essential and critical services may include prioritising the accessibility and affordability of telecommunications services to bridge digital divides, foster economic development, and enhance societal well-being. Proactively centring telecommunications as a reliable and inclusive resource empowers individuals and communities to fully participate in the digital age, while also safeguarding the continuity of vital services that depend on robust communication networks.	Developing (2) 
4.3 Communicate transparently with the public	Clear and timely updates regarding the nature and impact of disruptions, as well as steps being taken to restore services, are communicated to the public.	By fostering transparency, telecommunications entities build trust and credibility with the public, enabling informed decision-making and minimising uncertainty during challenging times. Effective communication ensures that customers and stakeholders are kept informed and empowered. Taking ownership of the problem, irrespective of the cause, is key.	Initial (1) 





Resilience Capabilities	Description of the Capability	Opportunity to Improve Sector Resilience	Current Sector Maturity Level
4.4 Raise resilience literacy	Individuals and communities are empowered by accessible and practical information.	By enhancing resilience literacy, the Australian public can better prepare for and respond to disruptions, thereby minimising their impact and overall recovery times. Investing in education and awareness initiatives enables communities to build resilience from the ground up, including via place-based solutions, fostering a culture of preparedness.	Developing (2) 
4.5 Build community participation and place-based solutions	Solutions are designed to be appropriate for local areas.	For example, solutions can be designed for community information hubs and limited-purpose networks to maintain EFTPOS functions during outages.	Developing (2) 
5. Shared responsibility			
5.1 Cultivate collaborative management	Collaborative management practices, such as promoting open communication and collaboration within and between telecommunications entities, enhance cooperation and knowledge-sharing.	A greater spectrum of stakeholders should be included and resourced for solution building. Mechanisms should be put in place to overcome commercial concerns around information sharing.	Developing (2) 
5.2 Establish a shared vision	Sectoral stakeholders, including telecommunications entities, regulatory bodies, and government agencies, are aligned towards common goals and objectives to build a shared vision. A shared vision fosters collaboration and cooperation, with public-private partnerships encouraging stakeholders to work together towards the collective advancement of the sector.	By defining clear objectives and priorities (such as enhancing service reliability, expanding coverage in underserved areas, and promoting digital inclusion), stakeholders collectively address challenges and seize opportunities. This shared vision not only ensures a more cohesive and unified approach to industry development but also reinforces the commitment to serving the broader interests of society.	Developing (2) 

Resilience Capabilities	Description of the Capability	Opportunity to Improve Sector Resilience	Current Sector Maturity Level
5.3 Enhance national data capability for near-real-time information sharing	Data infrastructure and capabilities at the national level are strengthened to facilitate secure and efficient data sharing among stakeholders within the Australian telecommunications sector, to enhance situational awareness and lessons management.	By prioritising data capability and data protection, near-real-time monitoring and reporting are facilitated across the sector. Appointing a national data custodian is one possible approach to building capability in data and information sharing.	Initial (1) 
5.4 Share information on the factors of risk and return information	Information on risk (including threats, threat sources, and vulnerabilities) and, where possible, expected returns among sector stakeholders are transparently shared.	Feedback loops should be closed multi-directionally, ensuring that, for example, information provided to the Australian Government yields returns that are shared with industry. This process enables stakeholders to gather insights from past experiences, fostering continuous improvement and informed decision-making.	Developing (2) 
5.5 Audit existing standards that make reference to resilience and harmonise standards nationally	Consistent resilience standards and/or guidelines across the nation are established through the identification and improvement of existing structures and standards. In turn, stakeholders can better ensure a unified approach to resilience planning and implementation.	Harmonisation through national standards and guidelines can simplify compliance efforts, promote interoperability, and facilitate information sharing among industry players, regulatory bodies, and government agencies.	Initial (1) 
6. Continuously learning and embedding lessons			
6.1 Whole-of-sector and cross-sector engagement	Purposeful cross-sector engagement allows for a broader perspective on emerging challenges and innovative solutions, ensuring that lessons learned are effectively integrated into policies and operations.	Collaboration across the entire sector, and with other critical sectors, should be fostered so stakeholders can share valuable insights, experiences, and best practices. Such collaboration promotes a culture of continuous improvement, enabling the telecommunications sector to adapt efficiently to an evolving risk horizon and opportunities.	Initial (1) 

Resilience Capabilities	Description of the Capability	Opportunity to Improve Sector Resilience	Current Sector Maturity Level
6.2 Consider and validate assumptions	Infrastructure planners, policymakers, and industry stakeholders unpack and test their assumptions about the resilience of infrastructure systems to potential threats and vulnerabilities within the sector.	By rigorously exposing and validating these assumptions, stakeholders can make more informed decisions and evidence-based resilience strategies. These may be achieved by employing tools such as scenario analysis, computational modelling, Delphi methods, and interdependency mapping.	Initial (1) 
6.3 Monitor network disturbances and disruptions and recover networks as appropriate	Building organisational and technical capability across the sector enables system performance monitoring in real-time. This proactive approach is complemented by clear and comprehensive guides, detailing the necessary technical and policy steps for network recovery in the event of a national or wide-scale outage.	These guides should be developed to go beyond the base requirement for telecommunications operators to 'restore to last known backup'. They should explicitly define 'data recovery objectives' and 'time recovery objectives' for various scenarios. This framework ensures that all operators have a standardised, well-understood approach to recovery, minimising confusion and improving efficiency during critical periods. The guides should be regularly updated to reflect technological advancements and evolving threats, and be integrated into operators' disaster recovery plans and industry-wide resilience strategies.	Initial (1) 
6.4 Analyse, learn, and formulate improvements	The sector is enabled to systematically analyse past events, identify patterns, and implement evidence-based improvements. The sector has whole-of-sector playbooks for consequence management, which are iterated and refined over time.	Historical feedback, data analysis, and potentially advanced technologies such as big data, and machine learning, should be leveraged to inform strategies for enhancing sectoral resilience.	Initial (1) 

Resilience Capabilities	Description of the Capability	Opportunity to Improve Sector Resilience	Current Sector Maturity Level
6.5 Stress test organisational response and exercise recovery capabilities	Exercises that stress test response plans help to establish best practices in disruption management, and build resilience.	Strategies to continually assess resilience and expose system vulnerabilities through whole-of-sector and cross-sector collaboration should be in place. Regular stress-testing exercises, including emergency drills, should be common practice.	<p>Developing (2)</p> 
7. Economic responsibility			
7.1 Resilience in investment decisions	This enables decision-makers to anticipate future market fluctuations and technological advancements. When unexpected events occur, it allows for financial resources to be reallocated toward projects that improve network redundancy, security, and flexibility; it also allows for a process of learning what strategies or solutions were effective.	Market trends and economic indicators should be monitored to inform decisions. Investments that enhance the ability of telecommunications infrastructure to withstand, adapt to, and recover from various disruptions should be prioritised.	<p>Developing (2)</p> 
7.2 Resilience in planning	The sector develops adaptive strategies for operational continuity and sustainability, integrating forward-thinking into a dynamic cycle of monitoring, anticipating, responding, and learning.	By effectively monitoring and analysing current conditions, organisations can anticipate and mitigate disruptions, leveraging predefined strategies to maintain operations. Post-incident, they can review outcomes to refine future planning, based on lessons learned	<p>Developing (2)</p> 

Resilience Capabilities	Description of the Capability	Opportunity to Improve Sector Resilience	Current Sector Maturity Level
7.3 Scalable solutions	Research and development investments are made to innovate new resilience technologies and methodologies, keeping the network ahead of emerging threats and vulnerabilities.	There should be investment in scalable technologies that can grow with demand, ensuring that the infrastructure remains robust and efficient as the network expands.	Developing (2) 
7.4 Resilience in domestic competition policy	Competition policy can be used as a means for promoting sector resilience.	Competition policy could be refined to support sector resilience by removing barriers to cooperation and collaboration among market players, specifically for resilience-enhancing activities, to alleviate concerns that cooperation and collaboration could be scrutinised under existing cartel laws, exclusive dealing or misuse of market power.	Initial (1) 
7.5 Resilience in telecommunications supplier diversity	Support for open technology standards, including existing initiatives like the Open RAN Principles endorsed by Australia, Canada, and the United States, involves investing in supplier development, domestic R&D capabilities, and international collaboration among allied nations.	<p>In response to increasing geopolitical competition, promoting a diverse and resilient telecommunications supply chain is crucial, influencing the development of future technologies such as 6G.</p> <p>Key strategies include leveraging next-generation technologies for supply chain management, fostering innovation through public-private partnerships, and implementing policies that incentivise research and resourcing in critical areas like quantum communications, and advanced network security.</p>	Developing (2) 








Resilience Capabilities	Description of the Capability	Opportunity to Improve Sector Resilience	Current Sector Maturity Level
7.6 Resilience rewards and incentives	Outcome-based regulation sets clear standards for acceptable service levels with financial penalties for failure to meet benchmarks. Technical prescriptions are proven and aligned with the sector's purpose. Ongoing reporting, including through scoring or rating systems, is clearly linked to improvements in consequence and incident management. Co-investment and co-design models with industry lead to continual improvement.	To incentivise greater economic responsibility, the government could provide coherent incentives, and rewards focused on mandating specific outcomes, prescribing performance metrics and/or technical means (as a last resort), and continually adjusting requirements based on ongoing monitoring and reporting.	Initial (1) 
7.7 Enhance adaptive capacity of supply chains	The supply chain can rapidly adapt to geopolitical events, market competition and unforeseen disruptions.	Supply chain continuity planning, diverse sourcing strategies, real-time visibility, predictive analytics, and incentives that promote innovation should be implemented.	Defined (3) 
 Overall assessment of the Australian telecommunications sector maturity against the Resilience Capabilities			 Developing 2

Resilience resources

Resilience resources are a prerequisite to strengthening the sector's resilience capacities and encompass the tangible and intangible assets necessary to support.⁴⁸ They encompass the tangible and intangible assets needed to support resilience.⁴⁹

Table 4 describes each resource and assesses the Australian Telecommunications Sector's current maturity against each resource.⁵⁰

Table 4. Assessment of Australian telecommunications sector maturity against resilience resources

Resource	Description	Current Sector Maturity Level
Financial resources	Funding and investment dedicated to resilience initiatives, including emergency funds and financial planning for unexpected disruptions from an all-hazards perspective.	Initial (1) 
Human capital	Skills, knowledge, and expertise of personnel crucial for implementing and sustaining resilience measures. Roles and responsibilities are clearly defined and continuously improved.	Developing (2) 
Infrastructure and technology	Physical assets and technological solutions that support resilient operations, including robust network infrastructure and advanced technologies for monitoring and response.	Defined (3) 
Data	Comprehensive and reliable data that informs risk assessments, decision-making processes, and real-time situational awareness.	Initial (1) 
Coordination mechanisms and processes	Sector-wide coordination mechanisms and processes exist to ensure that other available resources are leveraged for the purposes of resilience. These mechanisms and processes are continuously improved.	Developing (2) 
 Overall assessment of the Australian telecommunications sector maturity against the Resilience Resources		 Developing 2

48 Adapted from Rathnayaka, B, Siriwardana, C, Robert, D, Amaratunga, D & Setunge, S 2022, 'Improving the Resilience of Critical Infrastructures: Evidence-based Insights From a Systematic Literature Review', International Journal of Disaster Risk Reduction, vol. 78, <https://doi.org/10.1016/j.ijdrr.2022.103123>

49 Duchek, S 2019, *Organizational Resilience: A Capability-based Conceptualization*, BuR – Business Research, <https://doi.org/10.1007/s40685-019-0085-7>

50 Informed by evidence collected over the life of this project (compiled in Part 2 – Evidence in Support of Assessment).

2

Part 2 – Evidence in Support of the Assessment

In this section:

Step 1: Defining the sector

Step 2: Before disruption: Prepare and absorb: Situational awareness of the risk horizon

- Threats: What causes disruption
- Threat Sources: Who or what initiates a disruption
- Vulnerabilities: What makes the sector vulnerable to disruption

Step 3: During and post-disruption: Adapt, respond, recover: building consequence management capabilities

Step 4: Transforming from disruption: Lessons management integrates lessons across the phases of disruption management and works to mature sector resilience capabilities

Step 1: Defining the sector

TPDC definition of the telecommunications sector

The Australian telecommunications sector is a complex socio-technical system of entities, stakeholders, and assets, with the purpose of enabling communication to the intended recipient through the transmission, reception and/or delivery of information or data (**the Purpose**).

The assets that serve this purpose are tangible (e.g. a physical item, such as hardware, computing platform, network device, or other technology component) and intangible (e.g. human effort, data, information, software, capabilities, functions, services, intellectual property (trademarks, copyright patents), images, or reputation) (**Assets**).

These assets enable the delivery of communications (as data or voice signals) via services (carriage services, including cloud services) over networks, including physical or fixed networks, mobile or wireless networks (**Services**).

Entities are the individuals (persons), organisations, devices, or processes that underpin assets and the delivery of services (**Entities**).⁵¹

The sector is made up of stakeholders that provide these Services and/or Assets for the purpose, and their supply chains, as well as consumers and regulators (e.g. end-users, end-user organisations, supporters, developers, acquirers, suppliers, regulatory bodies, and people influenced positively or negatively by it) (**Stakeholders**).⁵²

How well the sector fulfils its purpose depends on sustaining a number of objectives (e.g. interconnectivity, continuity, availability, productivity, quality (speed, latency, priority) related to performance (**Performance**).

The sector's value is determined by stakeholders in consideration of loss of performance across the entire system life cycle or over a particular period. These value considerations have technical, organisational, social, economic, and national security dimensions (**Value**).⁵³

A summary of the types of entities and their function (with examples) in the Australian telecommunications sector is provided in Table 5.

51 Computer Security Resource Centre 2023, *FIPS 186-5 Digital Signature Standard (DSS)*, National Institute of Standards and Technology, <https://csrc.nist.gov/pubs/fips/186-5/final>

52 International Organization for Standardization 2015, *15288-2023 - ISO/IEC/IEEE International Standard - Systems and software engineering-- System life cycle processes*, <https://ieeexplore.ieee.org/document/10123367>

53 Ross, R, Pillitteri, V, Graubart, R, Bodeau, B & McQuaid, R 2021, *Developing Cyber-Resilient Systems: A Systems Engineering Approach*, National Institute of Standards and Technology, <https://doi.org/10.6028/nist.sp.800-160v2r1>

Defining the boundaries and elements of the telecommunications sector was a crucial first step in enhancing telecommunications resilience.

The following sections define the sector's key characteristics, dependencies and interdependencies, and relevant implications for resilience.

Unless otherwise indicated, the following information has been sourced from consultations with project stakeholders and the Expert Panel.

The sector is underpinned by competitive market dynamics

The Australian telecommunications market is characterised by the dominance of a select few major players. A small cluster of entrenched incumbents (i.e. Telstra, TPG Telecom, Optus) largely dictate market trajectories. They command significant market shares in providing wholesale and retail-level communications across all aspects of telephony and internet services, and wield considerable pricing leverage and influence over industry standards and information-sharing forums.⁵⁴ Several newer and challenger brands (InABox, Macquarie Telecom, MNF Group, Superloop, Southern Phones, TasmaNet and Vocus) have developed a footprint in recent years. In turn, the big three do not participate in industry-wide interconnection systems by not connecting to public internet exchange (peering) points.

The presence of NBN Co, which holds a wholesale monopoly over the National Broadband Network (the NBN) (intended to be a near-ubiquitous access network primarily for residential premises and other key sites across Australia) further impacts competition dynamics, as mass-market retail service providers must rely on its infrastructure to deliver broadband services, affecting their strategic options. Retail service providers to business and government customers are not compelled to use the NBN. Still, they must make their networks available on a wholesale basis, and regulated terms in certain circumstances if their networks can compete with the NBN.

Australia lacks a sovereign telecommunications equipment or software provider. Key network components are sourced from Cisco, Alcatel, Nokia, Ericsson, and Huawei (for 4G), software from Oracle, Cisco and Microsoft, and system integrators like IBM, Fujitsu and Accenture.

Small and medium providers (SMEs) (some of which are multi-national corporations in their own right, but with smaller Australian operations, or challenger brands), play a crucial role in fostering some diversity and innovation within the sector, offering tailored solutions for specific segments (i.e. Wi-Sky's rural broadband) or industries (i.e. AARNet's research and education services). Despite facing challenges such as regulatory costs and access to funding, SMEs contribute to competition by introducing new ideas, products, and business models. SMEs have concerns regarding the monopolistic tendencies of the big players, which create barriers to entry for market entrants.

Global over-the-top providers (OTTPs), such as Netflix, Amazon, and Spotify, have emerged as formidable competitors to traditional broadcasting, video and recording industry business models, offering digital content and services over telecommunications networks. Despite not owning last-mile telecommunications access network infrastructure, OTTPs leverage their extensive content libraries and innovative distribution models to capture a significant share of consumer attention and spending. OTTPs, including Google, Microsoft, and Meta, own massive amounts of global subsea cables, some of which terminate in Australia. Other OTTPs, including WhatsApp, Zoom, Teams, Cisco, and Twilio, have replaced traditional voice and messaging services.

These entities and stakeholders are outlined in Table 5 and include those not currently under the remit of telecommunications legislation. Categorical distinctions (e.g. between software providers and equipment manufacturers) are not as clear as the table may imply.

54 Australian Communications and Media Authority 2021, *Communications and media in Australia: Trends and developments in telecommunications 2022-2023*, https://www.acma.gov.au/sites/default/files/2023-12/Trends%20and%20developments%20in%20telecommunications%202022-23_0.pdf

Table 5. Summary of telecommunications entities and stakeholders, functions, and examples

Entity	Function	Example/s
Telecommunications carriers	Own and operate the infrastructure and networks used to transmit information	Telstra, Optus, TPG Telecom, Symbio, Vocus, Macquarie Telecom, Pivotal, Aussie Broadband, AARNet
Internet service providers (ISPs)	Provide access to the internet through telecommunications networks	iiNet, Aussie Broadband and Dodo Services, AARNet
Satellite providers	Provide satellite services.	Starlink, NBN Co SkyMuster (Optus Satellite), Amazon Project Kuiper, Pivotal.
Mobile network operators	Provide wireless communication services through cellular networks.	Telstra, Optus, TPG Telecom.
Mobile virtual network operators	Resellers of mobile networks under their branding.	Aldi, Exetel, Lebara, Tangerine.
Cable and satellite television providers	Transmit television programming through telecommunications networks.	Foxtel, VAST, Netflix, Disney.
Broadcaster	Transmit audio or visual content to a wide audience via radio, television or digital platforms.	Australian Broadcasting Corporation (ABC).
Equipment manufacturers	Produce the hardware and software used to transmit and receive information over telecommunications networks.	Cisco, Juniper, Arista, Alcatel, Nokia, Ericsson, and Huawei.
Software providers	Develop applications and software used to transmit and manage information over telecommunications networks.	Microsoft and Cisco.
Telecommunications infrastructure providers	Develop, construct, invest in, own and/or maintain telecommunications infrastructure assets.	BAI Communications, Field Solutions Group, and Waveconn.
Internet Exchange Point operators	Develop, construct, own and/or maintain infrastructure for the independent interconnection of internet networks operated by ISPs, enterprises, government and other organisations.	IAA, Megaport, Equinix.
System integrator	Design, install and maintain telecommunications infrastructure and systems for businesses and other organisations.	Fujitsu, IBM Australia and Accenture.

Entity	Function	Example/s
Cloud service providers	Offer cloud computing services to businesses and consumers.	Amazon Web Services, Microsoft Azure, Google Cloud Platform, Vault, and Macquarie Cloud Services.
Content Distribution Networks	Cloud-based providers who deliver aggregated content services.	Cloudflare, Fastly, Akamai
Communications as a service	Cloud-based providers who provide communications as a service over cloud infrastructure.	Microsoft Teams, Google Meetings, Zoom, Five9s.
Hosting Providers	Businesses providing the compute platforms for websites, business applications, etc.	Servers Australia, Webcentral, Digital Pacific.
Cyber-security companies	Provide security solutions for telecommunications networks and systems.	CyberCX, Macquarie Government, and SentinelOne
Wholesale network operators	Provide access to their networks and infrastructure to other service providers.	National Broadband Network (the NBN), Vocus Communications, Telstra, Optus.
Over-the-top content providers	Provide audio, video, and other digital content over telecommunications networks.	Netflix, Foxtel, Skype, WhatsApp, Stan, Spotify, and Apple Music.
Data centres and colocation providers	Provide facilities for hosting telecommunications equipment and infrastructure.	Equinix, NextDC, and Macquarie Data Centres.
Managed Service Providers	Design, build and operate networks on behalf of enterprises, government, and other organisations, using own and telecommunications carrier networks and equipment – Network As A Service (NAAS).	Nexon, Macquarie Telecom, Optus Business, Telstra, Megaport.
Private networks	Private telecom networks, owned by enterprises, universities, or institutions, use 5G/LTE and virtualised infrastructure to create secure, dedicated networks with unified connectivity, low latency, and high capacity within a specific area.	Ericsson, Vodafone and Nokia.

Entity	Function	Example/s
Regulatory bodies	Oversee and regulate the telecommunications sector to ensure fair competition, administer public resources used in telecommunications (spectrum, numbers, domain names), set technical standards, protect consumer interests, and promote public interest. There is also a level of international harmonisation through the International Telecommunications Union (ITU) and World Trade Organisation General Agreement on Tariffs and Trade (WTO GATS) commitments.	Australian Communications and Media Authority (ACMA), Australian Competition and Consumer Commission (ACCC), Telecommunications Industry Ombudsman (TIO), auDA Foundation.
Industry Associations	Advocate for industry, and in some cases, administer the co-regulation framework by establishing and managing industry Codes that set standards for industry performance.	Communications Alliance, Australian Mobile Telecommunications Association (AMTA), Communications Compliance, Internet Association of Australia (IAA).
Internet Governance organisations	Multistakeholder organisations that develop policies and manage shared internet identifiers: domain names, numbers and protocols, largely in the international space.	Internet Corporation for Assigned Names and Numbers (ICANN), Internet Engineering Task Force (IETF), Asia Pacific Network Information Centre (APNIC), auDA Foundation.
Australian Government	Regulates and oversees the industry to ensure that it operates fairly and competitively and promotes the development of telecommunications infrastructure and services for the benefit of consumers and businesses.	Department of Infrastructure, Transport, Regional Development, Communications and the Arts; the Department of Home Affairs; the National Emergency Management Agency.
State and territory governments, including emergency service organisations	Manage the licences and permits for the information media and telecommunications industry. Responsible for emergency management.	
Local councils	Play an important role in network facilities, and some own telecommunications infrastructure and have licences.	
Australian public	Consume and use telecommunications products.	
End Users	End users across critical infrastructure sectors.	

The sector provides services to a vast range of end-users

A systems approach encourages thinking of telecommunications infrastructure in its broader systemic context, including its perceived value to end users and their linkages with energy, transportation and financial infrastructures.⁵⁵

End-users of telecommunications range from the Australian public to critical sectors and businesses.⁵⁶

The way society uses networks and engages with the services it provides is constantly evolving. With this evolution comes increased demand, and an evolving demand profile. Telecommunications are the backbone of economic functions, enabling vital services such as online banking, e-commerce transactions, remote work capabilities, and digital communication platforms. These are all essential components of economic operations and societal functioning. Social media and streaming services have become deeply embedded in the day-to-day lives of people, particularly younger generations, serving as primary channels for communication, social interaction, and entertainment.

Telecommunications infrastructure serves as a lifeline for accessing essential services, particularly for marginalised communities, where it facilitates connectivity to healthcare, education, and government services. However, issues of access, affordability, and digital literacy persist, with disparities in connectivity hindering equal participation in the digital age.⁵⁷

As consumer expectations for uninterrupted connectivity continue to rise, the Australian telecommunications sector faces heightened pressure to deliver innovative solutions while upholding stringent data protection standards.

Technological innovation is evolving the market structure

As digitisation accelerates, sectors beyond traditional telecommunications providers are adopting characteristics that make them more similar to carriage services providers.

The Australian telecommunications landscape has transitioned from legacy circuit-switched networks to modern, highly complex and integrated packet-switched networks.⁵⁸ This evolution involves the adoption of advanced technologies, such as Internet Protocol (IP) networks, software-defined networking (SDN), and network function virtualisation (NFV).⁵⁹ These technologies enable the efficient routing, management, and delivery of data, voice, and multimedia services over converged or distributed networks.

In addition to core network infrastructure, the sector encompasses a wide range of distribution and access networks, including wired (i.e. copper terrestrial fibre-optic), wireless (i.e. mobile and satellite), broadcast (i.e. television and radio) networks, and submarine cables.

The sector depends on critical infrastructure, such as data centres and exchange facilities, as well as inter-exchange transmissions that link up these locations (see Figure 4 below). These networks underpin the seamless flow of digital information across national and international boundaries, serving varied communication needs, ranging from broadband internet access and mobile telephony to broadcasting and content delivery.

As other sectors, such as mining, agriculture and transport, integrate digital capabilities and rely more heavily on private data transmission and processing networks, their infrastructures and operations start mirroring those of traditional carriage service providers (CSPs) or carriers.

55 Andrew, T.N & Petkov, D 2003, 'The Need for a Systems Thinking Approach to the Planning of Rural Telecommunications Infrastructure', *Telecommunications Policy*, vol. 27, no. 1–2, [https://doi.org/10.1016/s0308-5961\(02\)00095-2](https://doi.org/10.1016/s0308-5961(02)00095-2)

56 Infrastructure Australia 2019, *An Assessment of Australia's Future Infrastructure Needs*, <https://www.infrastructureaustralia.gov.au/publications/australian-infrastructure-audit-2019>

57 Thomas, J, McCosker, A, Parkinson, S, Hegarty, K, Featherstone, D, Kennedy, J, Holcombe-James, I, Ormond-Parker L, & Ganley 2023, *Measuring Australia's Digital Divide: Australian Digital Inclusion Index: 2023*, ARC Centre of Excellence for Automated Decision-Making and Society, RMIT University, Swinburne University of Technology & Telstra, <https://doi.org/10.25916/528s-ny91>

58 Australian Communications and Media Authority 2021, *Communications and media in Australia: Trends and developments in telecommunications 2022-2023*, https://www.acma.gov.au/sites/default/files/2023-12/Trends%20and%20developments%20in%20telecommunications%202022-23_0.pdf

59 Bradai, A, Rehmani, M, Haque, I, Nogueira, M & Bukhari S 2020, 'Software-Defined Networking (SDN) and Network Function Virtualization (NFV) for a Hyperconnected World: Challenges, Applications, and Major Advancements', *Journal of Network and Systems Management*, vol. 28, no. 3, <https://doi.org/10.1007/s10922-020-09542-z>

This convergence blurs boundaries, with non-telecommunications entities becoming data carriers and network operators. For example, TransGrid has a large fibre network like many transport entities, and on-sells this network to telcos for general usage and has to maintain carrier licenses. Entities like Megaport operate Software Defined Networks (SDNs), or extensive networks, including internet exchange points, and perform many of the functions of a carrier, but may not need to align to the same regulations.⁶⁰

Substantial legacy infrastructure in networks necessitates continuous cycles of innovation

This hybrid infrastructure environment necessitates continuous innovation cycles and capital-intensive upgrades for providers to remain competitive and relevant.

The Australian telecommunications sector has substantial legacy systems amidst rapidly evolving technological change. Carriers and network operators must invest heavily in comprehensive network upgrades and workforce training to accommodate new technologies like SDN, 5G/6G, and beyond, while preserving integration and interoperability with legacy components.

The deployment of emerging technologies like artificial intelligence (AI) within network systems acts to stitch together legacy systems with new technologies.

Telecommunications is deeply interdependent with other critical infrastructure sectors

Crafting a resilience policy for the telecommunications sector necessitates consideration of the interconnected nature of critical infrastructure systems. This poses a challenge due to the absence of a fully comprehensive understanding of Australia's critical infrastructure interdependencies.

The telecommunications sector is deeply interconnected with other sectors, forming a complex web of cross-sector dependencies and interdependencies.⁶¹

One of the primary dependencies is on the energy sector, as communication networks require a continuous and reliable power supply to operate. Telecommunications infrastructure, including network equipment, data centres, and cell towers, relies on electric power for operation and backup generation during power outages. Similarly, the telecommunications sector enables efficient power supply through remote monitoring and control of electrical infrastructure, facilitating real-time management of power grids. Telecommunications also supports the deployment of smart grid technologies and energy management systems.

Telecommunications services are critical for operating other essential services, such as banking, emergency services, transportation, and healthcare. Financial institutions rely on telecommunications networks for real-time transactions and data exchange. At the same time, emergency services depend on reliable communication channels to operate emergency hotlines, coordinate responses, and disseminate information, especially during disruption.

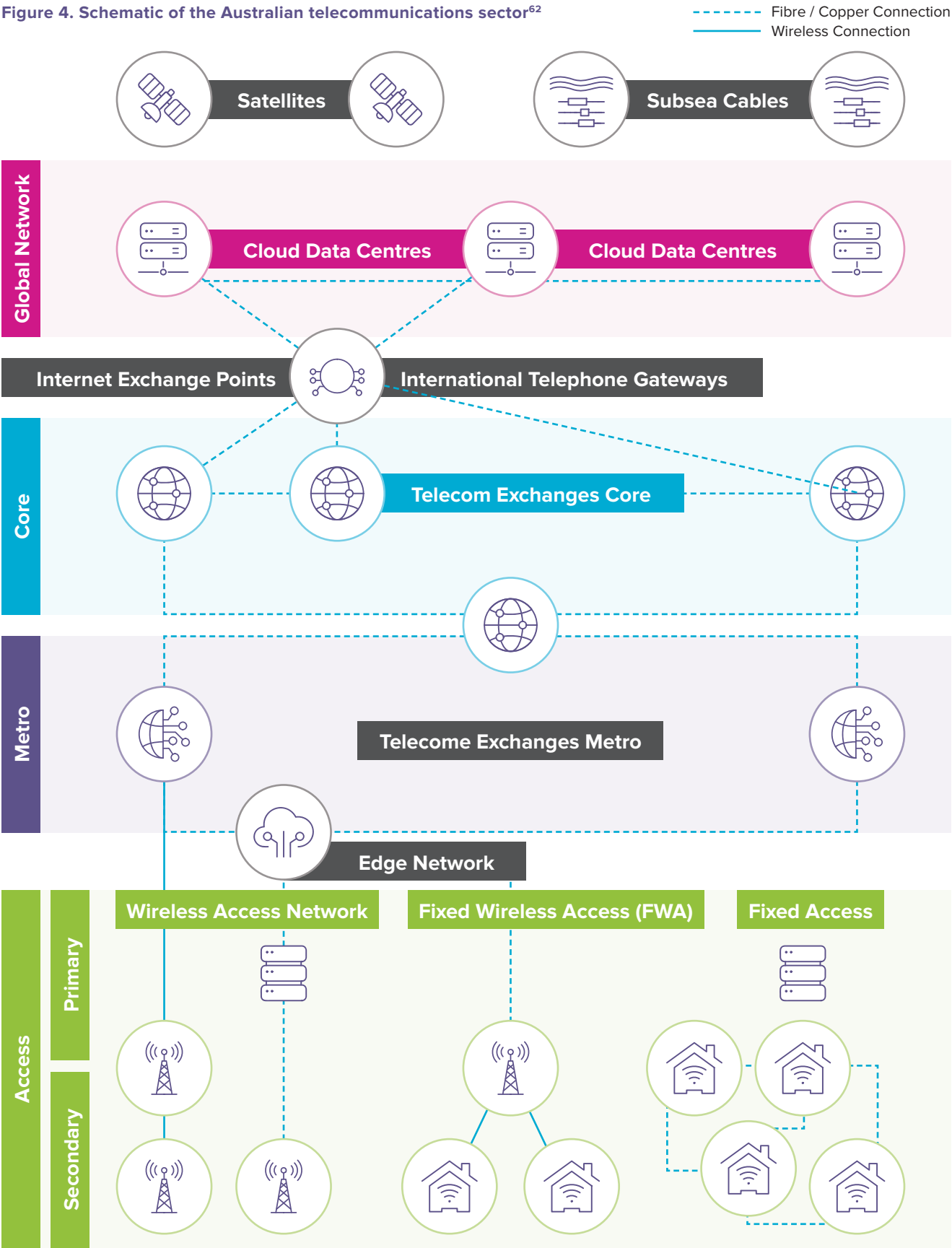
Transportation systems use telecommunications technologies for traffic management and signalling, vehicle tracking, and passenger communication. The transportation sector plays a vital role in delivering diesel fuel to power backup generators, enabling the continuation of backup telecommunications services during outages.

The telecommunications sector serves as a linchpin that supports and enables the functioning of various sectors of the economy and society. However, it also relies on other sectors to facilitate its assets and services.

⁶⁰ The key legal difference between a CSP and a carrier is whether the entity owns and operates equipment for the supply of carriage services to the public. Those who own and operate the equipment used to provide services to the public are required to hold a carrier licence. Whereas those who provide services across infrastructure provided by others (even leased lines) are not carriage service providers until they provide services to the public but are not required to hold any licence to do so. They are, however, subject to a significant amount of technical regulation as carriage service providers. These concepts are all defined in the Telecommunications Act.

⁶¹ Rinaldi, S, Peerenboom, J & Kelly, T 2001, 'Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies', IEEE Control Systems, vol. 21, <https://doi.org/10.1109/37.969131>

Figure 4. Schematic of the Australian telecommunications sector⁶²



62 Adapted from: Gatti, S & Chiarella, C 2020, *The Evolution of the Telecom Infrastructure Business*, Disruption in the Infrastructure Sector: Challenges and Opportunities for Developers, Investors and Asset Managers, <https://doi.org/10.1007/978-3-030-44667-3>

The sector is internationally interconnected

An inter-woven web of international dependencies exposes Australian telecommunications to a range of geopolitical, economic, and operational challenges external to its control.

Beyond domestic settings, international interdependencies are crucial for global connectivity and data exchange.

Subsea cables, spanning vast distances across oceans, form the backbone of international communication networks, enabling high-speed data transmission between continents. These cables are essential for facilitating international trade, financial transactions, and global collaboration, underpinning the interconnected nature of the digital economy.

The sector relies on a complex range of multiple international suppliers for sourcing equipment, components, and technologies critical for infrastructure development and network expansion. With no domestic manufacturing capabilities for many telecoms inputs, Australia's resilience hinges on the continuity and security of these global supply lines, including considering the mitigation plans that all foreign-owned suppliers have in place. Collaborative efforts and partnerships on a global scale are essential for ensuring the resilience, security, and interoperability of telecommunications networks in an increasingly interconnected world.

International standards are pivotal to ensuring interoperability across global telecommunications networks. These standards, established by international organisations such as the Internet Engineering Task Force (IETF), International Telecommunication Union (ITU) and the Institute of Electrical and Electronics Engineers (IEEE), are continually negotiated by global stakeholders. They facilitate the compatibility of different manufacturers' equipment and technologies, enabling smooth operation and efficient data exchange.

Regulation is fragmented

Resilience capabilities have to be embedded across the regulatory structure. This is a challenge in a sector where responsibility for continuity of service lies between the private sector and government, and within different arms of government.⁶³

The Australian telecommunications sector has varied regulatory underpinnings and objectives, including the focus on the ability to mitigate risk, ensure competition, and/or perform to certain standards, ensure universally available basic levels of service, and protect consumers. These ensure trade-offs between access to and service availability at a certain quality and price.

The Australian telecommunications sector is subject to regulation by several key government agencies, including:

- Australian Communications and Media Authority (ACMA)
- Australian Competition and Consumer Commission (ACCC)
- Department of Infrastructure, Transport, Regional Development, Communications and the Arts
- Department of Home Affairs.

These regulatory bodies oversee various aspects of the telecommunications sector, including licensing, spectrum management, consumer protection, security, and competition policy.

The *Telecommunications Act 1997* (Telecommunications Act) serves as the primary legislative framework governing telecommunications regulation, outlining obligations for telecommunications providers regarding service quality, accessibility, and privacy protection.

63 Ampratwum, G, Osei-Kyei, R & Tam, V 2022, 'Exploring the Concept of Public-private Partnership in Building Critical Infrastructure Resilience Against Unexpected Events: A Systematic Review', *International Journal of Critical Infrastructure Protection*, vol. 39, <https://doi.org/10.1016/j.ijcip.2022.100556>

The *Telecommunications Act* is supplemented by further key legislation that expands upon how the sector is regulated:

- *Radiocommunications Act 1992*, sets out the spectrum regulatory framework
- *Telecommunications (Interception and Access) Act 1979*, contains obligations of telecommunications companies to support law enforcement efforts
- *Telecommunications (Consumer Protection and Service Standards) Act 1999*, establishes the universal services regime and the consumer service guarantees
- *Competition and Consumer Act 2010*, contains telecommunications sector-specific competition rules and access regime.

In line with the 2023-2030 Australian Cyber Security Strategy, the Australian Government plans to transfer the Telecommunications Sector Security Reforms (TSSR) from Part 14 of the *Telecommunications Act* to the *Security of Critical Infrastructure (SOCI)* Act. This move aims to consolidate security regulations and streamline obligations under a unified Telecommunications Security and Risk Management Program (TSRMP) within the SOCI Act.⁶⁴

The NBN is subject to specific regulatory arrangements to ensure equitable access to high-speed broadband services nationwide.⁶⁵

The National Emergency Management Agency, state and territory governments, and local councils play a role in other domains, such as permits and emergency management.

The telecommunications sector in Australia has historically been governed by policies aimed at maintaining market competition.⁶⁶ Other regulatory paradigms include regulating consumer protection (i.e. the *Telecommunications Consumer Protections Code* and the Telecommunications Industry Ombudsman), or technical standards (i.e. those made by ACMA under s376 of the *Telecommunications Act* about specified customer equipment or specified customer cabling).

Current enterprise resilience objectives optimise technical efficiency

Resilience aims to strengthen the sector's capacities through capability-building measures that stimulate and incentivise cooperation and innovation to resolve resilience issues, encouraging continuous improvement across all stakeholders within the sector.

Telecommunications networks have been optimised technically for efficiency at steady-state capacity with a small margin (headroom) to accommodate for daily demand fluctuations.⁶⁷ The benefit to the public is high efficiency at a lower cost.

To maintain performance, enterprises make trade-offs between the technical, organisational, social, and economic dimensions of resilience.

Technical, organisation, economic, and social dimensions could reinforce one another and be thought of as ways to sustain or constrain performance loss, restore performance, and improve performance.

Engaging with these dimensions is the key to building capabilities to mature resilience capacities across the sector.⁶⁸

64 King & Wood Mallesons 2024, *Strengthening Australian Critical Infrastructure Against Cyber Risks*, <https://www.kwm.com/au/en/insights/latest-thinking/strengthening-australias-critical-infrastructure-against-cyber-risks-consultation-on-legislative-reforms-close-1-march-2024.html>

65 Department of Infrastructure, Transport, Regional Development, Communications and the Arts n.d., *NBN legislative framework*, <https://www.infrastructure.gov.au/media-technology-communications/internet/national-broadband-network/nbn-legislative-framework>

66 Howell, B & Potgieter, P 2020, 'Politics, Policy and Fixed-line Telecommunications Provision: Insights From Australia', *Telecommunications Policy*, vol. 44, <https://doi.org/10.1016/j.telpol.2020.101999>

67 Owen, R 2024, Broadband Technology Research Unit (BTRU) at University of Technology Sydney (Faculty of Engineering and Information Technology), private correspondence. Modern networks employ dynamic resource allocation allowing them to adapt to varying demands flexibly. Headroom can vary significantly depending on the network, region, service type, time of day and provider.

68 Kozine, I & Andersen, H 2015, *Integration of Resilience Capabilities for Critical Infrastructures Into the Emergency Management Set-up*, Safety and Reliability of Complex Engineered Systems, CRC Press, https://backend.orbit.dtu.dk/ws/files/128948305/Paper_ESREL_2015_postprint.pdf

Enterprise resilience arises from the dynamic interaction between the following:

- technical level, including capabilities that ensure network reliability, fault tolerance, and recovery methods⁶⁹
- organisational level, including capabilities to ensure business continuity during and after disruptions⁷⁰
- economic level, including capabilities encouraging economic return on investment and environmental sustainability⁷¹
- social level, including capabilities that strike a balance between the diverse needs of end-users, accessibility, and fostering industry innovation.⁷²

As the sector becomes increasingly integral to modern society, there's a growing question as to how to bring these components of the system together, and whether current trade-offs promote innovation to prepare the country for future challenges.

69 Cholda, P, Tapolcai, J, Cinkler, K, Wajda K & Jajszczyk, A 2009, 'Quality of Resilience as a Network Reliability Characterization Tool', *IEEE Network*, vol. 23, no. 2, <https://doi.org/10.1109/MNET.2009.4804331>

70 Patriarca, R, Di Gravio, G, Costantino, F, Falegnami, A & Bilotta, F 2018, 'An Analytic Framework to Assess Organizational Resilience', *Safety and Health at Work*, vol. 9, <https://doi.org/10.1016/j.shaw.2017.10.005>

71 Coscelli, A & Thompson, G 2022, *Resilience and Competition Policy: Economics Working Paper*, Competition and Markets, GOV.UK, <https://www.gov.uk/government/publications/resilience-and-competition-policy-economics-working-paper>

72 Kozine, I & Andersen, H 2015, *Integration of Resilience Capabilities for Critical Infrastructures Into the Emergency Management Set-up*, Safety and Reliability of Complex Engineered Systems, CRC Press, https://backend.orbit.dtu.dk/ws/files/128948305/Paper_ESREL_2015_postprint.pdf

Step 2: Prepare and absorb: Situational awareness of the risk horizon

TPDC definition of threat

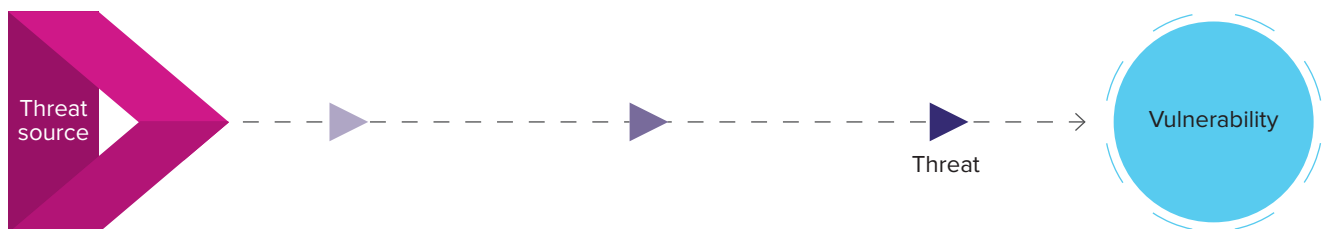
A threat in the telecommunications sector is a potential source of disruption or harm that, when exploited through a vulnerability, could lead to undesirable consequences. Threats require an initiating source (a threat source) to become active.⁷³

TPDC definition of threat source

A threat in the telecommunications sector necessitates the presence of an agent⁷⁴ to initiate its manifestation into a disruptive event. In other words, a threat requires an initiating source to become active. A threat source may be malicious (i.e. terrorists, foreign state actors, insiders, or criminals) or non-malicious (i.e. unintentional, accidental, natural, emerging phenomena and/or technology).⁷⁵

TPDC definition of vulnerability

A vulnerability is a condition determined by physical, social, economic, and environmental factors or processes that increase the susceptibility of an individual, a community, assets, or systems, to the impacts of threats.⁷⁶ Within telecommunications assets, systems and services, a vulnerability is a weakness in system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.⁷⁷



73 Branagan, M 2012, 'A Risk Simulation Framework for Information Infrastructure Protection' PhD thesis, Queensland University of Technology, https://eprints.qut.edu.au/51006/1/Mark_Branagan_Thesis.pdf

74 Branagan, M 2012, 'A Risk Simulation Framework for Information Infrastructure Protection' PhD thesis, Queensland University of Technology, https://eprints.qut.edu.au/51006/1/Mark_Branagan_Thesis.pdf

75 Ibid.

76 United Nations Office for Disaster Risk Reduction 2007, *Vulnerability*, Sendai Framework Terminology on Disaster Risk Reduction, <https://www.undrr.org/terminology/vulnerability>

77 Montgomery, D, Polk, T, Ranganathan, M, Souppaya, M, NIST, Barker, W, Dakota Consulting 2020, 'Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD) - Volume B: Approach', Architecture, and Security Characteristics, NIST Special Publication 1800-15B, <https://www.nccoe.nist.gov/sites/default/files/legacy-files/iot-ddos-nist-sp1800-15b-draft.pdf>

A key part of building sector resilience is developing situational awareness of the risk horizon before disruption occurs.

This step refers to the sector's ability to mitigate, prepare and absorb disruption. This capacity is sustained by having situational awareness of the risk horizon.⁷⁸ This entails understanding the risk factors, including threats, threat sources, and vulnerabilities.⁷⁹

By comprehensively understanding the risk horizon, entities can enhance their capacity to effectively prepare for disruptions. This awareness enables proactive measures to strengthen absorption capacity, allowing the sector to better withstand shocks without significant degradation of services. It may also facilitate adaptation by identifying emerging threats and changes in advance, enabling timely adjustments to operational strategies and systems.

Implications of risk management for consequence management

During disruptions, heightened situational awareness also enhances consequence management.⁸⁰ Informing resource allocation and prioritisation enables better facilitation of the response and recovery phases, including the swift restoration of critical services.

Implications of risk management for lessons management

Ongoing situational awareness supports continuous learning from past disruptions, fostering a culture of resilience, and driving transformational improvements in the sector's systems and processes over time.⁸¹ It includes governance processes to enable the sector to respond to, learn from, and transform, after disruptive events.

Thus, situational awareness plays a pivotal role in maturing resilience capacities across all phases of disruption management, ultimately ensuring the sector's ability to thrive amidst ever-evolving challenges.

The subsequent sections offer an overview of the risk factors necessary to form situational awareness, providing a collation of evidence provided by project stakeholders.

Threats: What causes disruption?

"While it's important to get a good picture of what the status quo is, we also want to be looking forward – to the next 2, 5, 10, 20 years. What will the threats be to the resilience of the telco sector then?"

The TPDC Threat Taxonomy

Different sector stakeholders report on the strategic threat horizon in different ways. They use different terminology and focus on different concerns (variously and contradictorily defined as risks, threats, and hazards).

To profile threats at the sector-level, a common lexicon was required. The TPDC Threat Taxonomy was developed, based on extensive consultation, and a literature review of international threat taxonomies, to establish the required common lexicon.⁸²

Figure 5 provides an overview of the categories within the TPDC Threat Taxonomy.

78 Cavallo, A 2013, 'Integrating disaster preparedness and resilience: a complex approach using System of Systems', *Australian Journal of Emergency Management*, vol. 29, no. 3, <https://knowledge.aidr.org.au/resources/ajem-jul-2014-integrating-disaster-preparedness-and-resilience-a-complex-approach-using-system-of-systems/>

79 Branagan, M 2012, 'A Risk Simulation Framework for Information Infrastructure Protection' PhD thesis, Queensland University of Technology, https://eprints.qut.edu.au/51006/1/Mark_Branagan_Thesis.pdf

80 Wirtz, J 2013, *What Just Happened? Situational Awareness, Threat Characterization, and Effective Consequence Management*, Palgrave Macmillan US eBooks, https://doi.org/10.1057/9781137336439_2

81 Su, W &, Junge, S 2023, 'Unlocking the Recipe for Organizational Resilience: A Review and Future Research Directions', *European Management Journal*, vol. 41, <https://doi.org/10.1016/j.emj.2023.03.002>

82 Appendix B details the methodology for development of the TPDC threat taxonomy.

Figure 5. Project evidence mapped against TPDC Threat Taxonomy categories

Threats		
Physical	Cyber & Technology	Climate & Environment
<ul style="list-style-type: none">Power failureDamage to fibre-optic cablesFailure of infrastructure or equipmentTheft and other criminal damage	<p>Cyber:</p> <ul style="list-style-type: none">Foreign interference and espionageGeopolitical conflictData breachesCriminal activityDDoS attacksSpectrum interference and jamming <p>Tech:</p> <ul style="list-style-type: none">Software malfunction and misconfigurationNetwork congestionLegacy hardware and failure	<ul style="list-style-type: none">BushfiresFloodsLightningHeavy rainSolar flares and space weather
Economic	Regulatory	Supply Chain
<ul style="list-style-type: none">Investment allocationInfrastructure resourcing at the state and local levelsSkills gaps and shortages	<ul style="list-style-type: none">Regulatory changesRegulatory non-complianceSanctions	<ul style="list-style-type: none">Disruption to supply chainsEspionage and foreign interferenceGlobal market demands

In the following sections, evidence collected during this project was applied to the TPDC Threat Taxonomy to build the following threat profile of the Australian telecommunications sector as at June 2024.

Physical threats

Threats in this category may be related to property, including loss or theft, destruction, sabotage, or vandalism. They may also be related to physical systems, including electrical and structural facilities, water distribution, sanitation, natural gas, or electronic media.

The project’s Expert Panel and sector stakeholders identified a spectrum of physical threats:

- power failure
- damage to fibre-optic cables
- failure of telecommunications infrastructure or equipment
- theft and other criminal damage.

Table 6. Physical threats identified by stakeholders

Threat	Evidence
Power failure	<p>The uninterrupted power supply was paramount to ensure that telecommunications infrastructure, including communication towers, exchanges, hubs network equipment, and data centres, have a reliable electricity supply. Power disruptions directly impact service availability.</p> <p>Climate change further strains the country's aging electrical infrastructure, exacerbating the stress on the grid and amplifying power outage occurrences.⁸³</p> <p>Lack of understanding about energy-telecom interdependencies impeded coordinated mitigation.</p> <p>The Trusted Information Sharing Network's Communications Sector Group was actively working with the Energy Sector Group to explore issues between these interdependent sectors. However, while existing efforts, such as the 2020 Memorandum of Understanding (MoU) between these sectors, aimed to improve collaboration and knowledge-sharing, they have not led to meaningful change.⁸⁴</p> <p>Stakeholders have suggested that understanding the threat of power failure required recognising the importance of power autonomy and the wide range of available technologies, from conventional methods like mobile emergency diesel generators to elective vehicle fleets and off-grid microgrids.</p>
Failure of telecommunications infrastructure or equipment	<p>This encompassed various scenarios, from minor glitches to critical failures, and affected individual hardware elements, such as transmission lines, signal repeaters, and network switches. These faults could render entire systems inoperable and disrupt the transmission and routing of data across telecommunication networks, impacting service continuity and reliability.</p> <p>Key drivers included inadequate maintenance practices, insufficient monitoring systems, and a lack of proactive measures to identify and address potential issues before they escalated.</p> <p>Industry stakeholders voiced concerns regarding the failure to learn from past infrastructure or equipment failures and implement lessons into practice. For instance, the Warrnambool Exchange fire, triggered by an unspecified electrical fault, illustrated this. The incident caused extensive damage to critical communications equipment, resulting in widespread service outages and disruptions for businesses, emergency services, and the wider community, given the exchange's role as a transmission hub connecting approximately 100,000 people across South-West Victoria, spanning about 15,000 square kilometres.⁸⁵</p> <p>Despite a number of reports and inquiries following the incident, which emphasised the need for greater proactive maintenance and more robust real-time monitoring systems, similar occurrences persisted.</p> <p>Aging infrastructure and technological obsolescence further exacerbated the risk of equipment failure as networks evolved. Older equipment required increased monitoring and additional spare parts that can be difficult to source and maintain. The rapid pace of technological advancement also renders older equipment incompatible with newer systems, complicating networks, maintenance and upgrades.</p>

83 Perera, A, Nik, V, Chen, D, Scartezini, J & Hong, T 2020, 'Quantifying the Impacts of Climate Change and Extreme Climate Events on Energy Systems', *Nature Energy* vol. 5, <https://doi.org/10.1038/s41560-020-0558-0>

84 Energy Networks Australia 2020, *Memorandum of Understanding (MoU) between Energy Networks Australia and Communications Alliance*, <https://www.energynetworks.com.au/news/ena-and-comms-alliance-mou/>

85 Gregory, M, Scholfield, K, Ahmed, K, McLaren, D & Williams, J 2014, 'Warrnambool Exchange Fire - Resilience and Emergency Management', *Journal of Telecommunications and the Digital Economy*, vol. 2, <https://doi.org/10.7790/ajtde.v2n4.72>

Threat	Evidence
Damage to fibre-optic cables	<p>Undersea cables carry 98% of global data traffic. Inadvertent severing from ship anchors and fishing nets threatens undersea cables. Australia has subsea cable protection zones, which aim to restrict maritime activities that could damage cables while enforcing substantial penalties for cable damage.⁸⁶</p> <p>Deliberate damage to cable integrity is a growing concern, encompassing the potential for destruction or tampering by malicious threat sources, such as non-state actors or state adversaries. Non-state threat sources have recently increased, with many terrestrial fibre-optic cables being cut in the search for copper cables.</p> <p>Terrestrial fibre-optic cables are susceptible to damage from excavation activities, with incidents often arising from individuals failing to adhere to safety protocols such as 'before you dig'. In these cases, cables may be inadvertently severed during construction or excavation work, resulting in widespread service outages, severing network redundancy, and costly repairs for telecommunications providers. On occasion, cable strikes have been caused by construction crews, who face civil penalties.</p> <p>Australian Government stakeholders have identified several root causes of cable damage, including inadequate cable marking, insufficiently deep trenches, and a lack of effective monitoring systems.</p> <p>Industry views suggested that the root causes of threats to telecommunications infrastructure included a lack of public awareness, insufficient proactive enforcement of protection zones by relevant authorities (e.g. state harbour masters), and inadequate penalties for accidental damage.</p>
Theft and other criminal damage	<p>Australia still maintains its copper cable network, although there has been a significant shift towards upgrading to fibre optic infrastructure with the rollout of the NBN. Copper cables, battery backups, and generators for mobile phone towers are often stolen from telecommunications infrastructure.</p> <p>These thefts impact service continuity while imposing costly repairs for providers, estimated between \$30,000 and \$60,000 per incident. The costs do not reflect the service disruption to the public, government, and emergency services, and the associated brand damage.</p> <p>Whilst the above attacks are motivated by monetary gain, the industry has also seen an increase in malicious targeted attacks on telecommunications infrastructure. For example, since 2018, malicious attacks motivated by anti-5G sentiments have escalated. Since 2023, several monopole towers have been sabotaged, causing structures to fail or collapse. These caused service disruption to the immediate service areas. Replacing towers or equipment is costly.</p> <p>Industry stakeholders identified insufficient deterrents, such as penalties under federal and state criminal laws, as a primary contributing factor to this threat. They argued that penalties should reflect such disruptions' severe business and public impacts.</p> <p>On the other hand, some government stakeholders argued that the responsibility for safeguarding infrastructure lies with telecommunications providers.</p>

86 Clare, M 2021, *Submarine Cable Protection and the Environment*, International Cable Protection Committee (ICPC), https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/ICPC_Public_EU_March%202021.pdf

Gaps

The below threat was not identified by project stakeholders or was only briefly acknowledged, despite broader literature indicating their importance to situational awareness of the current risk horizon:

- broader interdependencies.

Table 7. Gaps in physical threat evidence identified by the project team

Threat	Description
Broader interdependencies	Aside from energy interdependency, the Australian telecommunications sector has overlooked other critical physical interdependencies, such as the geographic concentration of telecommunications equipment. ⁸⁷ The clustering of infrastructure in certain geographical areas makes it susceptible to localised disruptions caused by accidents, malicious activities, or climactic events. Alternative solutions may require multiple towers in sites that face a lower threat level of disruption, but this may increase cost. Therefore, incorporating considerations of physical interdependencies beyond energy supply is imperative for enhancing the sector's preparedness and resilience against a diverse range of threats.

Cyber and technology threats

Threats in this category may be related to hardware, software and systems, including hardware capacity, performance, maintenance and obsolescence, software compatibility, configuration management, change control, cyber security, development and coding practices, and testing.

The project's Expert Panel and sector stakeholders identified a spectrum of cyber and technology threats.

- **Cyber threats** primarily involve unauthorised access or attacks directed at computer systems, networks, and data, necessitating measures to preserve information confidentiality, integrity, and availability.
- **Technological threats** can be broader, encompassing threats associated with telecommunications hardware and software that facilitate the processing and transmission of information (e.g. misconfiguration).

Cyber threats

Project stakeholders perceived an excessive focus by the government on broad 'cyber incidents' by malicious actors targeting critical telecommunications assets and networks, given their role in storing sensitive information, sustaining vital services, and maintaining extensive connectivity with other entities and infrastructure sectors.

Internationally, a diverse array of malicious cyber actors, including state and state-sponsored entities, cybercriminal syndicates, and issue-driven groups, have exhibited both the motivation and capability to target critical infrastructure for various purposes, encompassing service disruption, data exfiltration, and cyber espionage.⁸⁸

87 Rinaldi, S, Peerenboom, J & Kelly, T 2001, 'Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies', *IEEE Control Systems*, vol. 21, <https://doi.org/10.1109/37.969131>

88 Australian Signals Directorate 2023, *ASD Cyber Threat Report 2022-2023*, <https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf>

Table 8. Cyber threats identified by stakeholders

Threat	Evidence
Geopolitical instability and conflict	Geopolitical instability and conflicts may amplify cyber threats to the Australian telecommunications sector by increasing the likelihood of state-sponsored attacks, intelligence gathering, and cyber-criminal activities. These threats are further compounded by the potential for misinformation campaigns over carriage services and retaliatory cyber-attacks in response to economic sanctions.
Foreign interference and espionage	<p>Foreign interference and espionage pose significant threats that extend beyond mere disruption to the Australian telecommunications sector. These activities can have far-reaching implications, including jeopardising national security, undermining economic interests, and compromising individual privacy.</p> <p>Parts of the telecommunications sector – such as OTTPs – are often the primary conduit for foreign interference and espionage. For example, the <i>Senate Select Committee on Foreign Interference through Social Media's Final Report</i> (2023) stated that 'foreign interference is now Australia's principal national security threat which risks significantly undermining our values, freedoms and way of life'.⁸⁹</p> <p>Hostile foreign actors, including state-sponsored entities and cyber espionage groups, target telecommunications infrastructure to gain unauthorised access to sensitive information, compromise network integrity, and disrupt critical communications systems. These adversaries may exploit vulnerabilities in telecommunications networks to conduct espionage activities, such as intercepting sensitive communications or stealing proprietary technology and intellectual property.</p> <p>Additionally, foreign interference efforts aim to manipulate or sabotage telecommunications systems to undermine national sovereignty and advance geopolitical agendas. The clandestine nature of these activities makes them challenging to detect and mitigate effectively, highlighting the need for robust cybersecurity measures, threat intelligence sharing, and close collaboration between government agencies and telecommunications providers to safeguard against such threats.</p>

89 Senate Select Committee on Foreign Interference through Social Media 2023, *Final Report of the Select Committee on Foreign Interference Through Social Media*, https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/pubs/rp/rp2324/Quick_Guides/ForeignInterferencethroughSocialMedia

Threat	Evidence
Data breaches	<p>Australian telecommunications entities handle vast amounts of customer data, including personal information, billing records, and communication metadata. The sector has faced high-profile data breaches in recent years, such as the 2022 Optus data breach, where personal details of around 10 million Australians were exposed.⁹⁰</p> <p>These incidents have significantly eroded consumer trust in telcos as customers become increasingly wary of how their personal information is handled and protected.⁹¹ Breaches also serve as enablers for cyber criminals and nation-states to misuse the breached data for further cyber incidents, such as the misuse of login and password combinations, identity theft, and fraud.</p> <p>Security experts have suggested reforming data retention laws to limit how long telecommunication companies must keep sensitive information. They also advocate for giving ex-customers the right to request data deletion. There also needs to be limits on what is collected in the first place by implementing smarter mechanisms to validate identity.</p> <p>Some industry stakeholders believed consumers should be able to sue companies directly over data breaches, rather than relying solely on the industry regulator. There were calls for the government to implement stricter penalties for companies that failed to adequately protect customer data. Rebuilding consumer trust would require telcos to prioritise robust cybersecurity measures and transparent communication regarding data protection practices.</p>
Criminal activity, including malware and scams	<p>Malware and scams pose an ongoing threat to the Australian telecommunications sector, targeting both the infrastructure and the end-users. Cybercriminals deploy sophisticated malware to infiltrate networks, disrupt services, and steal sensitive information, compromising the integrity of communications. Increasingly, new unique malware is generated by AI. Additionally, phishing scams and social engineering attacks exploit human vulnerabilities, tricking users into revealing personal data or installing malicious software. These threats may lead to widespread service disruptions, financial losses, and a significant erosion of consumer trust. The pervasive and evolving nature of these cyber threats highlights the ongoing risk to the security and reliability of Australia's telecommunications services.</p> <p>Prevention of these issues is quickly becoming an element that providers need to manage, whether by streamlining user identification to prevent identity theft and SIM swapping, or through technical controls, like filtering and threat blocking, as per the 2023-2030 Australian Cyber Security Strategy.⁹²</p>

90 Kaye, B 2022, *Australia's Optus says up to 10 million customers caught in cyber attack*, Reuters, <https://www.reuters.com/technology/australias-optus-says-up-10-mln-customers-caught-cyber-attack-2022-09-23/>

91 Roy Morgan 2022, *A Majority of Australians Have No Trust in Telcos*, <https://www.roymorgan.com/findings/a-majority-of-australians-have-no-trust-in-telcos>

92 Department of Home Affairs 2023, *2023–2030 Australian Cyber Security Strategy*, <https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf>

Threat	Evidence
DDoS attacks	<p>DDoS attacks can overwhelm network infrastructure with a flood of malicious traffic. When left unaddressed, these attacks cause significant service disruptions, render websites and online services inaccessible, and lead to substantial operational and financial impacts. The volume and sophistication of modern DDoS attacks can strain even the most robust defences. Such disruptions not only affect service providers, but also undermine consumer confidence and trust in the reliability of telecommunications services.</p> <p>There have been DDoS attacks that have exploited vulnerabilities in telecommunications systems to attack other organisations.⁹³ The increasing frequency and scale of DDoS attacks underscore the need for effective mitigation strategies to protect Australia's critical telecommunications infrastructure.</p>
Spectrum interference and jamming	<p>Spectrum interference and jamming can disrupt wireless communications and degrade the quality of service and hardware. Intentional jamming and unintentional interference can affect critical services, including emergency communications, leading to significant operational challenges. Uncompliant signal boosters used by customers can degrade service for other network users.⁹⁴</p> <p>These disruptions can result in dropped calls, reduced data speeds, and complete service outages, impacting both consumers and businesses. The increasing reliance on wireless technologies makes the sector particularly vulnerable to these threats, highlighting the need for robust spectrum management and interference detection measures, to ensure reliable and secure telecommunications services.</p>

Technological threats

Table 9. Technological threats identified by stakeholders

Threat	Evidence
Software malfunctions	<p>Software malfunctions can stem from bugs, outdated software, compatibility issues, and misconfigurations. The complexity of modern telecommunications networks, integrating various software systems for billing, customer management, and network operations, amplifies the risk of malfunctions.</p> <p>Incidents of software failures can result in service outages, degraded performance, and security vulnerabilities, leading to significant operational and financial repercussions, including loss of customer trust and regulatory penalties. Misconfiguration issues can arise from human errors during network setup, maintenance, or updates, the complexity of networks, lack of automation, inadequate training, and rapid changes without proper testing and validation.</p> <p>As technology rapidly advances, more frequent updates and patches are necessitated, which, if not managed correctly, can introduce new errors.</p>

⁹³ Australian Signals Directorate 2023, *ASD Cyber Threat Report 2022-2023*, <https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf>

⁹⁴ Bennett, M 2015, *Illegal Mobile Phone Signal Boosters Causing Problems for Other Network Users*, ABC News, <https://www.abc.net.au/news/2015-03-07/mobile-repeaters-disrupting-mobile-phone-signal/6287256>

Threat	Evidence
Legacy hardware and hardware failure	<p>Typical operational technologies (OT) used across the telecommunication sector tend to have long usage lifespans, and many run outdated and increasingly vulnerable software. If connected to the Internet (e.g. for remote management), the legacy OT may be exposed to cyber threats as it is difficult to patch legacy hardware and software without disrupting business continuity. Due to equipment age, general component failure, electrical supply issues, or geomagnetic storms, hardware failure may also disrupt telcos and their services.</p>
Network congestion and spectrum allocation	<p>Network congestion is exacerbated by the increasing demand for data and higher performance requirements and affects all networks and network operators. With more users streaming content, engaging in online gaming, utilising telehealth services, and working remotely, the need for sufficient spectrum and spectrum management has never been greater. Shortages or delays in spectrum allocation can lead to severe congestion, resulting in slower speeds and reduced service quality, especially during peak usage times. This congestion not only frustrates consumers but also hampers the efficiency of businesses that rely on fast and reliable internet connections.</p> <p>Many stakeholders emphasised that as the IoT continues to grow, the risk of congestion will only increase with more devices connected to the network. This necessitates ongoing investment in network upgrades, including the expansion of 5G and 6G infrastructure, to accommodate the ever-growing data traffic and ensure the long-term resilience and competitiveness of the telecommunications sector.</p> <p>Project stakeholders indicated that conducting a post-mortem investigation is crucial to uncovering the root causes of software failures and implementing effective countermeasures. However, current approaches to investigating such failures often prioritised restoring normal operations swiftly, leaving systems vulnerable to recurring issues.</p>

Gaps

The below threats were not identified by project stakeholders or were only briefly acknowledged, despite broader literature indicating their importance to situational awareness of the current risk horizon:

- hybrid warfare
- software misconfiguration
- evolving technologies, including artificial intelligence, automation, and 6G.

Table 10. Gaps in cyber and technology threats identified by the project team

Threat	Description
Hybrid warfare	<p>The Australian government identified hybrid warfare as an emerging threat of concern.⁹⁵ This includes potential cyber espionage activities conducted by nation-state actors against critical infrastructure, such as telecommunications networks. However, industry stakeholders did not address this threat during our consultations, despite its salience in government discussions.</p> <p>Governments have a heightened awareness of this threat in light of strategic electronic warfare involving critical infrastructure in war-stricken countries, such as Ukraine and Palestine.⁹⁶</p> <p>Additionally, advisories released by agencies including CISA, NSA, FBI, and Five Eyes partners in February and March 2024, warned of state-sponsored actors compromising and maintaining persistent access to critical infrastructure in the United States.⁹⁷</p>
Software misconfiguration	<p>Software misconfigurations represent a significant yet frequently underestimated threat to the resilience of telecommunications networks.⁹⁸ Despite their prevalence, many entities – government and industry alike – do not recognise the commonality and severity of software misconfigurations, resulting in a dangerous underestimation of the associated risk. Automation can be a positive in this area. Reliance on a small pool of experts to create system configurations and then automation to manage it may heighten the chance of failure, especially if the pool of experts is not available.</p> <p>This threat involves incorrect settings or unchanged default configurations, which can create exploitable weaknesses in software systems. Disruptions attributed to software misconfigurations are often underreported, obscuring the true extent and impact of the issue. Issues in configuration (i.e. Domain Name System (DNS) configuration, Border Gateway Protocol (BGP) and Network Time Protocol (NTP)) are generally common causes of network disruption. This underreporting can lead to a lack of awareness and insufficient preparedness, thereby increasing the susceptibility of systems to catastrophic outages or cyber incidents that exploit these seemingly simple but critical errors.</p>
Evolving technologies, including artificial intelligence, automation and 6G	<p>The emphasis on present threats rather than emerging ones may leave the sector unprepared for the future complexities advanced technologies will bring. The sector's focus on immediate and well-known threats, like cyber incidents and data breaches, has overshadowed the potential risk associated with emerging technologies. AI and automation could enable sophisticated cyber incidents that outpace current defence mechanisms.⁹⁹ Additionally, 6G, with its promise of unprecedented connectivity and speed, introduces new vulnerabilities that are not yet fully understood.¹⁰⁰</p>

95 Australian Signals Directorate 2023, *ASD Cyber Threat Report 2022-2023*, <https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf>

96 Australian Signals Directorate 2023, *ASD Cyber Threat Report 2022-2023*, <https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf>

97 The Cybersecurity and Infrastructure Security Agency, National Security Agency, Federal Bureau of Investigation, Australian Signals Directorate's Australian Cyber Security Centre, Canadian Centre for Cyber Security, New Zealand National Cyber Security Centre, Computer Emergency Response Team New Zealand, & National Cyber Security Centre 2023, *2022 Top Routinely Exploited Vulnerabilities*, Cybersecurity and Infrastructure Security Agency, <https://www.cisa.gov/news-events/alerts/2023/08/03/cisa-nsa-fbi-and-international-partners-release-joint-csa-top-routinely-exploited-vulnerabilities>

98 GSMA 2020, *Mobile Telecommunications Security Threat Landscape*, <https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2020/02/2020-SECURITY-THREAT-LANDSCAPE-REPORT-FINAL.pdf>

99 Balmer, R, Levin, S & Schmidt, S 2020, 'Artificial Intelligence Applications in Telecommunications and Other Network Industries', *Telecommunications Policy*, vol. 44, no. 6, <https://doi.org/10.1016/j.telpol.2020.101977>

100 Nguyen, V, Lin, P, Cheng, B, Hwang, R & Lin, Y 2021, *Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges*, IEEE Communications Surveys and Tutorials 23, <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9524814>

Climate and environment threats

Threats in this category may be related to environmental or climatic conditions, including fire, flood, cyclone, storm, hurricane, heat, snow, earthquake, pollution, dust, radiation, space weather, wildlife, and pandemic.

The Project's Expert Panel and sector stakeholders identified a spectrum of climate and environment threats.

- The sector is concerned about threats it has encountered previously, such as bushfires, floods, lightning and storms, and heavy rain.
- The sector is concerned about threats it has little to no experience with, such as solar flares and space weather.

Table 11. Climate and environment threats identified by stakeholders

Threat	Description
Bushfires, floods, lightning, storms, and heavy rain	<p>Australia has recently experienced a series of consecutive and compounding disruptions driven by climate and environmental conditions. Recent significant events have included:</p> <ul style="list-style-type: none"> • 2019-20 Black Summer bushfires, which impacted 1390 telecommunications facilities. Of all the facilities impacted, 51% experienced outages of four hours or more, while 26% experienced outages of less than four hours. The remaining 23% of facilities were impacted but did not experience any outages.¹⁰¹ • 2022 East Coast floods, which impacted 802 commercial telecommunications carrier sites in NSW alone, and created outages across fixed line, mobile and internet services, with some communities becoming completely isolated. Most site outages were restored within two weeks.¹⁰² • 2023 Queensland storms, which caused communities in Mount Maria and several suburbs near Agnes Water to have no mobile services for nearly two weeks.¹⁰³ • 2024 Cyclone Kirrily, which caused widespread loss of telecommunications services.¹⁰⁴ • 2024 Northern Territory floods, which caused communication problems between police, fire and emergency services in Darwin and those in flood-affected Borroloola.¹⁰⁵ • 2024 Victorian storms, which cause prolonged phone and internet outages, including a loss of access to Triple Zero services.¹⁰⁶

¹⁰¹ Australian Communications and Media Authority 2020, *Impacts of the 2019-20 bushfires on the telecommunications network*,

<https://www.acma.gov.au/publications/2020-04/report/impacts-2019-20-bushfires-telecommunications-network>

¹⁰² New South Wales Government 2022, *2022 NSW Flood Inquiry*, https://www.nsw.gov.au/sites/default/files/noindex/2022-08/VOLUME_TWO_Full%20report.pdf

¹⁰³ Queensland Reconstruction Authority 2024, *2023-24 South Queensland Severe Storms*, <https://www.qra.qld.gov.au/2023-24-South-Queensland-Severe-Storms>

¹⁰⁴ Queensland Reconstruction Authority 2024, *Tropical Cyclone Kirrily: the northern system that became a statewide disaster event*, <https://www.qra.qld.gov.au/news-case-studies/case-studies/tropical-cyclone-kirrily-northern-system-became-statewide-disaster-event>

¹⁰⁵ Vivian, S & Bardon, J 2024, *ADF has airlifted 380 Borroloola residents to Darwin as McArthur River hits flood peak*, ABC News, <https://www.abc.net.au/news/2024-03-22/borroloola-flood-mcarthur-river-adf-evacuation/103619244>

¹⁰⁶ Tippet, H 2024, *Victoria's power outage caught thousands by surprise — here's how it happened*, ABC News, <https://www.abc.net.au/news/2024-02-14/victoria-melbourne-power-outage-storms-how-did-it-happen/103464714>

Threat	Description
<i>Bushfires, floods, lightning, storms, and heavy rain continued</i>	<p>The sector widely acknowledged the critical role of telecommunications to deliver timely warnings and information to communities during times of disruption. A loss of these services – either via network congestion, as people contact emergency services, family and friends, by direct damage, or by loss of power – can impede informed decision-making, such as evacuation timing.</p> <p>Moreover, the centrality of telecommunications to the provision of other essential services – such as ATMs and EFTPOS services, and relatedly, purchasing food and fuel – creates cascading impacts for communities affected by climate and weather events.¹⁰⁷</p> <p>More Australians than ever are being impacted by climate and environmental threats. For example, in 2022, nearly 70% of Australians lived in an area covered by a natural disaster declaration.¹⁰⁸ Even under a relatively optimistic low-emissions scenario, Australia's cost of natural disasters in Australia is estimated to grow to \$73 billion per year by 2060.¹⁰⁹</p> <p>The climate outlook for Australia is concerning. The <i>State of the Climate Report</i>,¹¹⁰ found:</p> <ul style="list-style-type: none"> • an increase in the intensity of heavy rainfall events, with further intensification of this phenomenon in areas of the country as the climate warms • an increase in extreme fire weather and in the length of the fire season across large parts of the landmass, especially the south and east, and an increase in the number of days experiencing dangerous fire weather • Australia is projected to continue to get hotter into the future, with more extremely hot days and fewer extremely cool days • Australia's cool season rainfall is projected to decrease across many regions of the south and east, likely leading to more time spent in drought • fewer tropical cyclones are projected, but a greater proportion of those that occur are projected to be of high intensity, with ongoing large variations from year to year. <p>There is, therefore, a pressing need for the sector to further improve its readiness for the inevitability of these threats materialising as disruptive incidents.</p>

107 Binskin, M, Bennett, A & Macintosh A 2020, *Royal Commission into National Natural Disaster Arrangements Report*, Commonwealth of Australia, <https://www.royalcommission.gov.au/system/files/2020-12/Royal%20Commission%20into%20National%20Natural%20Disaster%20Arrangements%20-%20Report%20-%205Baccessible%5D.pdf>

108 KPMG 2023, *70 Percent of Australians Impacted by Natural Disasters*, <https://kpmg.com/au/en/home/media/press-releases/2024/09/70-percent-of-australians-impacted-by-natural-disasters.html>

109 CSIRO 2022, *State of the Climate 2022*, CSIRO, <https://www.csiro.au/en/research/environmental-impacts/climate-change/State-of-the-Climat>

110 Ibid.

Threat	Description
Extreme space weather	<p>The threat of extreme (G5) space weather events is of significant concern for project stakeholders, especially as there has not been an event of this magnitude in the digital age. Geomagnetic storms of G5 level can potentially disrupt critical infrastructure such as power grids, causing power outages and satellite services, affecting communications and global position, navigation and timing services that use high-frequency radio communication.</p> <p>Scientific projections suggest an impending solar maximum around 2025, indicating heightened magnetic activity on the sun and the potential for solar flares and coronal mass ejections (CMEs).¹¹¹ Relatedly, in May 2024, a severe (G4) geomagnetic storm was experienced, without disruptions to Australian telecommunications services.¹¹²</p> <p>Despite difficulties in predicting solar cycles, the detection of a CME provides only a brief window – typically less than 12 hours – before its potential impact on Earth is felt, with less than an hour available to assess the event's severity.</p> <p>These events can disrupt satellite signals, crucial for communication and GPS systems, and disrupt satellite integrity, potentially leading to the loss or degradation of satellite networks. Moreover, the vulnerability of long-distance undersea cables, essential for global internet connectivity, to large-scale storms, remains poorly understood, amplifying concerns over potential disruptions in communication and internet services – and the potential for Australia to be cut off from the rest of the world.¹¹³</p> <p>These findings underscore the need for further research, proactive planning, and all-hazards consequence management practices to mitigate the potential impact of space weather on the telecommunications sector.</p>

¹¹¹ The European Space Agency 2024, *The May 2024 Solar Storm: Your Questions Answered*, ESA, https://www.esa.int/Space_Safety/Space_weather/The_May_2024_solar_storm_your_questions_answered

¹¹² National Aeronautics and Space Administration (NASA) 2020, *Solar Cycle 25 Is Here. NASA, NOAA Scientists Explain What That Means*, NASA, <https://www.nasa.gov/news-release/solar-cycle-25-is-here-nasa-noaa-scientists-explain-what-that-means/>

¹¹³ Weule, G 2022, *Just How Bad Could a Big Solar Storm Be in the Internet Age? And How Would Australia Be Affected?*, ABC News, <https://www.abc.net.au/news/science/2022-03-01/solar-storm-risks-power-network-internet/100812978>

Gaps

The below threats were not identified by project stakeholders or were only briefly acknowledged, despite broader literature indicating their importance to situational awareness of the current risk horizon:

- failure to learn from past events
- pandemic.

Table 12. Gaps in climate and environment threats identified by the project team

Threat	Description
Failure to learn from past events	Despite multiple Royal Commissions and other inquiries, lessons regarding climate and environmental disruptions have not necessarily been fully integrated into policy and planning frameworks within the telecommunications sector. Often, responses to these disruptions remain reactive rather than proactive, with a tendency to address immediate concerns rather than implement long-term strategies to mitigate future risk. This reactive approach not only jeopardises the resilience of telecommunications infrastructure, but also comes with significant costs, both in terms of financial expenditures and societal impacts. There is a critical need for a shift towards proactive measures that incorporate lessons learned from past inquiries to better safeguard telecommunications infrastructure and services against future disruptions, while also minimising the economic and social costs associated with reactive responses.
Pandemic	Despite recent experiences with COVID-19 and the growing body of literature ¹¹⁴ indicating the likelihood of more frequent and severe pandemics in the future, stakeholders in the telecommunications sector overlooked the pandemic as a potential threat in their consultations. This omission raises questions about whether there is an assumption that lessons from past pandemics, such as the COVID-19 crisis, were sufficiently learned and integrated into resilience planning, or if there is a belief that the likelihood of experiencing another pandemic is minimal. However, given the unpredictable nature of infectious disease outbreaks and their significant impacts on the capacity demands of telecommunications networks, pandemic preparedness must remain a key component of risk and resilience strategies at the enterprise and government levels.

Economic threats

Threats in this category may be related to economic and market conditions, including inflation and deflation, market access, availability of materials and equipment, labour supply and skills availability, market structure, ownership and control, trade orientation, and technological level.

The Project's Expert Panel and sector stakeholders identified a spectrum of economic threats:

- investment allocation
- infrastructure resourcing at the state and local level
- skills gaps and shortages
- competition policy and its relationship to resilience.

¹¹⁴ Marani, M, Katul, G, Pan, W & Parolari, A 2021, 'Intensity and Frequency of Extreme Novel Epidemics', *Proceedings of the National Academy of Sciences of the United States of America*, vol. 118, <https://doi.org/10.1073/pnas.2105482118>

Table 13. Economic threats identified by stakeholders

Threat	Evidence
Investment allocation	<p>Major players in the Australian telecommunications sector consistently reported facing a widening gulf between industry revenues and the substantial capital outlays required to meet growing data usage demands.</p> <p>This dynamic raises questions over investment responsibilities and where the onus of responsibility falls: is this the private sector's job, or is state intervention warranted to safeguard resilience as a national strategic priority?</p> <p>In economic terms, there is a divergence between the level of investment that is commercially optimal and that which is optimal from the perspective of resilience as a national strategic priority. There is a lack of valuation of the value of reliability, which makes quantification of any investment gap difficult, and makes setting attendant policy settings to address the incentives issue difficult.</p> <p>Providers grappled with complex investment allocation decisions, weighing resilience initiatives against competing priorities like network expansion, technological upgrades, and shareholder obligations. Without incentive structures or regulatory guidance, short-term commercial pursuits may take precedence over long-term investments. Negative customer perceptions of mitigation efforts and limited industry incentives hinder progress and investment in infrastructure upgrades.</p> <p>The telecommunications sector faces commercial hurdles, and lack of commercial incentives to improve resilience, impacting service delivery and innovation.</p> <p>The sector has not drawn effective links between infrastructure upgrades and other outcomes, such as economic growth. Knowledge of, and investment in particular use cases (particularly 5G use cases) is not occurring systematically, meaning that benefits are not accruing to agriculture, mining, and other sectors. The cost associated with identifying, communicating, and implementing beneficial technologies is higher than earlier standardised technologies with broad applications.</p> <p>Underinvestment is evident in certain regions, with rural and remote areas lacking access to essential mobile network technology (e.g. 4G), highlighting disparities in infrastructure development. This reflects a divergence between commercially viable investments rather than economically and socially desirable infrastructure.</p> <p>With a limited number of established enterprises wielding substantial market power, competition within the sector is intense, yet constrained, within defined boundaries. Another issue is that no one network provider has the capacity to fully service the entire market, which constrains incentives to compete in non-metropolitan markets.</p>

Threat	Evidence
Infrastructure resourcing at the state and local level	<p>State and territory governments are pivotal in resource allocation and local deployments. Inconsistencies in infrastructure prioritisation, funding mechanisms, and resilience standards across jurisdictions could impede the sector's ability to develop unified, cohesive resilience capabilities across the continent.</p> <p>The lack of cohesion in the division of responsibilities between federal and state/territory bodies and the private sector in emergency response and critical infrastructure protection adds further complexities in coordinating during disruptions.</p> <p>State governments often lack ownership and resources to mitigate risks associated with telecommunications infrastructure, impacting service reliability and resilience.</p> <p>There is an urgent need for vertical integration of resilience planning and response, emphasising the importance of cohesive strategies spanning from federal to local government levels. Collaboration between telecommunications and energy sectors remains a missed opportunity for coordinated planning and response efforts.</p>
Skills shortages and capacity constraints	<p>Labour market dynamics, particularly the lack of a pipeline of telecommunications engineers, result in shortages of skilled personnel to rebuild telecommunications infrastructure post-disruption. Persistent skills shortages undermine the overall capacity of the sector to operate effectively, resulting in underperformance across all areas of design, build and operations, as well as flawed outsourcing decision-making.</p> <p>At a broader level, there are limitations in Australia's overall approach to technology assessment that could act to guide better government decisions about resilient infrastructure planning. Public funding initiatives, primarily grant-based with shared financial commitments, may lead to misaligned incentives and reliance on taxpayer support for infrastructure upgrades.</p>

Gaps

The below threat was not identified by project stakeholders or was only briefly acknowledged, despite broader literature indicating their importance to situational awareness of the current risk horizon:

- competition policy and its relationship to resilience.

Table 14. Gaps in economic threats identified by the project team

Threat	Description
Competition policy and its relationship to resilience	<p>Within the sector, it is unclear how the aims of competition policy intersect with resilience.¹¹⁵</p> <p>Amongst many goals, competition policy aims to foster a diverse supply ecosystem and consumer choice. However, it can inadvertently create more fragmentation with reduced incentives for coordinated activity, particularly in a shared threat environment. Major telecommunications providers are reluctant to engage in cooperation or collaboration because of fears of anti-competitive behaviour.</p> <p>This reluctance belies the fact there are many instances (e.g. during the pandemic) in which competitive dynamics were put aside to ensure continuity of service. However, there is an everyday understanding that the regulatory structure prevents cooperation, even though exemptions can be sought from the ACCC when business planning activities are in the public interest.</p> <p>There is a ‘first-mover’ advantage for those companies that can demonstrate activities that confer resilience. Equally, there is the potential for ‘free-riding’, in that one operator can benefit from the resiliency-increasing activities of another without taking action themselves.¹¹⁶</p> <p>Within individual organisations, there is a lack of understanding that commercial decisions made at the enterprise level, while rational and efficient, do not give rise to sectoral resilience, due to interdependencies with other stakeholders.</p> <p>To enable resilience there needs to be a clearer sense of how competition policy, and its interpretation for commercial purposes, might be aligned to lead to better sectoral capabilities and outcomes. The danger for operators is that prescriptive network requirements may be pushed on them, or potentially onerous administrative responsibilities, or regulatory penalties. In this context, penalties would need to be high enough to offset the savings of opting not to build resilient infrastructure, even given the financial difficulty that a significant outage may cause.</p>

¹¹⁵ Gannon, J, Tendulkar, A, Lim, C & Serentschy, G 2023, *Lessons for Canada From International Approaches to Network Resiliency and Reliability*, International Telecommunications Society (ITS), <https://www.econstor.eu/bitstream/10419/277962/1/Gannon.pdf>

Coscelli, A & Thompson, G 2022, *Resilience and Competition Policy: Economics Working Paper, Competition and Markets*, GOV.UK, <https://www.gov.uk/government/publications/resilience-and-competition-policy-economics-working-paper>

¹¹⁶ Coscelli, A & Thompson, G 2022, *Resilience and Competition Policy: Economics Working Paper, Competition and Markets*, GOV.UK, <https://www.gov.uk/government/publications/resilience-and-competition-policy-economics-working-paper>

Regulatory threats

Threats in this category may be related to legal and regulatory conditions, including: regulatory compliance, legislation, litigation, intellectual property, consumer protection, health and safety, taxation, privacy, and data security.

The Project’s Expert Panel and sector stakeholders identified a spectrum of physical threats:

- regulatory changes
- regulatory non-compliance
- regulatory sanctions.

Table 15. Regulatory threats identified by stakeholders

Threat	Evidence
Regulatory changes	<p>The current regulatory framework falls short in regulating resilience, and recently announced regulatory changes may not push the sector towards being more resilient.</p> <p>Currently, cyber security requirements for telecommunications providers are found in both the <i>Telecommunications Act</i> and the <i>SOC/ Act</i>. To avoid duplication and reduce complexity for telecommunications providers who operate in multiple critical infrastructure industries, the 2023-2030 Cyber Security Strategy indicates that these obligations are to be consolidated within the <i>SOC/ Act</i>. The new obligations would include registering critical infrastructure assets, using government assistance measures, and cyber security incident reporting.¹¹⁷</p> <p>However, many stakeholders across the sector are concerned that this consolidation could add unnecessary regulatory strain, rather than promote accountability and resilience.</p> <p>Designed with a prescriptive and compliance-focused approach, the <i>SOC/ Act</i> primarily emphasises the protection of assets, rather than ensuring the continuity and resilience of essential services these assets provide.</p> <p>Critical infrastructure operators are required to follow the frameworks identified in the Act to mitigate risks relating to data theft, foreign interference, and national security. However, the Act tends to overlook the societal elements of resilience, neglecting considerations, such as social cohesion and the broader impacts of telecommunications disruptions on communities and individuals.</p> <p>It remains unclear how the <i>SOC/ Act</i> will effectively enhance resilience and prevent incidents such as the 2023 Optus outage, which resulted from a network misconfiguration and was not a cyber event. As pointed out by network architects involved in the project, the Act doesn't require or establish standardised measures that could have mitigated or reduced the impact of the Optus outage, like implementing proper network segmentation, testing for complete failure scenarios, or developing essential skills to swiftly recover networks during crises.</p>

117 Department of Home Affairs 2023, 2023–2030 Australian Cyber Security Strategy, <https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf>

Threat	Evidence
Regulatory changes continued	<p>Furthermore, any regulatory focus on asset protection may result in a fragmented approach to resilience, where efforts are primarily directed towards safeguarding specific infrastructure components, rather than ensuring the resilience of the entire telecommunications system and its interdependent sectors.</p> <p>Similarly, following the Optus outage in 2023, industry commentary has intensified regarding the appropriate reporting mechanisms to the government for incident management versus regulatory response.</p> <p>Within the sector, there is a prevailing sentiment that government assistance measures might overestimate the technical capabilities of government agencies to assist in cases of technical failure.¹¹⁸ Particular references were made to the so-called "step-in rights" outlined in the 2023-2030 Cyber Security Strategy, which empowers the government with last-resort consequence management powers. While this view underscores scepticism about government intervention in technical matters, it is important to acknowledge other perspectives that advocate for a collaborative approach between industry and government to ensure effective incident management and regulatory oversight in the face of disruptions.</p>
Regulatory non-compliance	<p>The burden of compliance with regulatory requirements can be substantial, leading to increased operational costs and administrative burdens for these enterprises. In the telecommunications sector, both small and large businesses face the challenge of moral hazard, where the costs of a company's behaviour (like underinvesting in network redundancy) are borne by others (e.g. customers or the broader economy when services fail).¹¹⁹</p> <p>Compliance standards need to strike a balance: too lax, and big players might avoid investing in measures; too strict and small providers might struggle to comply. Encouraging all providers, big and small, to invest in resilience capacities as a commercial differentiator, not just as a cost, has merit.</p> <p>This burden often includes investing in specialised personnel, technology, and resources to ensure adherence to complex regulatory frameworks. While regulations typically aim to safeguard consumer interests, ensure network security, and maintain industry standards, the cost of compliance can sometimes outweigh the benefits, especially for SMEs with limited resources.</p> <p>As a result, regulatory non-compliance not only exposes telecommunications providers to legal ramifications such as penalties, but also hampers their ability to innovate, compete effectively, and provide quality services to customers. Therefore, striking a balance between regulatory oversight and the practical realities SMEs face, is crucial to fostering a resilient telecommunications sector.</p>

118 Department of Home Affairs 2023, *2023–2030 Australian Cyber Security Strategy*, <https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf>

119 Hansson, I & Skogh, G n.d., 'Moral Hazard and Safety Regulation', *The Geneva Papers on Risk and Insurance*, vol. 12, <https://www.jstor.org/stable/41950219>

Threat	Evidence
Regulatory sanctions	<p>Global sanctions are increasing yearly, reflecting a backdrop of increasing geopolitical tensions.¹²⁰</p> <p>In 2018, the Australian government issued security guidance related to the Telecommunications Sector Security Reforms (TSSR) emphasising the risk of involving third-party vendors in 5G networks that might be subject to foreign government directives conflicting with Australian law. This guidance had significant repercussions for the telecommunications sector, notably excluding major vendors like Huawei from the market. As a result, Australian telecommunications entities had to find alternative suppliers for the roll-out of 5G technologies, potentially delaying deployment and increasing costs.¹²¹</p> <p>Moreover, the backdrop of increased geopolitical tensions raises concerns about the potential for future sanctions targeting other telecommunications equipment providers. Such sanctions could disrupt supply chains, limit technological advancements, and heighten geopolitical tensions, further jeopardising the stability and competitiveness of Australia's telecommunications sector.</p>

Supply chain threats

Threats in this category may be related to dependencies, including supplier viability, logistics provision, including over-reliance, route disruption, provider failure, technology services.

The Project's Expert Panel and sector stakeholders identified a spectrum of supply chain threats:

- disruption of supply chains
- software supply chains
- espionage and foreign interference
- global market demands.

¹²⁰ World Economic Forum 2024, *Global Risks Report 2024*, <https://www.weforum.org/publications/global-risks-report-2024/in-full/global-risks-2024-over-the-limit/>

¹²¹ Morrison, S, Fifield, M & Australian Government 2018, *Government Provides 5G Advice to Australian Carriers*, https://parlinfo.aph.gov.au/parlInfo/download/media/pressrel/6164495/upload_binary/6164495.pdf;fileType=application%2Fpdf#search=%22media/pressrel/6164495%22

Table 16. Supply chain threats identified by stakeholders

Threat	Evidence
Disruption of supply chains	<p>The telecommunications sector relies on complex global supply chains.</p> <p>The dependence on foreign suppliers and vendors exposes the country to disruptions. Combined with rising costs and inflationary pressures, supply chain disruptions create challenges for telecommunications providers to maintain profitability, while investing in next-generation network technology.</p> <p>Global suppliers of network equipment have a high degree of visibility of their supply chains. They are advocates for investment in next-generation technology (AI, 5G and quantum computing) because of the effects these technologies have on realising cost efficiencies and enabling outcomes, like better monitoring of industrial decarbonisation efforts.</p> <p>Over the pandemic era, consumers' increased demand for smartphones, wi-fi modems, gaming hardware and IoT sensors created subsequent demand for chipsets from global equipment manufacturers. These manufacturers also experienced chip shortages due to the COVID-19 pandemic, which required redistribution of chipset supply to enterprise customers.</p> <p>Global supply chains can be weaponised, causing significant disruptions. The procurement of key components can be influenced by geopolitical conflicts, affecting the stability and reliability of the supply chain.</p>
Software supply chains	<p>Historically, supply chain incidents have targeted trusted relationships by compromising an insecure supplier to infiltrate their larger trading partners. Today, the greater concern is software supply chains. The pervasive adoption of open-source software in telecommunications infrastructure is not immune to security breaches, despite often scrupulous code review by the open-source community. Open-source code, while beneficial for innovation and cost-efficiency, can be a target for malicious actors who exploit known vulnerabilities. Open-source code can also be inappropriately deployed injudiciously and without the intended constraints to its use. Proprietary source code can similarly be opaque to scrutiny and is dependent on the provider to rectify and remediate source code issues.</p> <p>In addition, the overall complexity of software means interdependencies and capabilities can be hard to identify, and source code and systems review are inherently difficult.</p>
Espionage and foreign interference	<p>High reliance on components, software, and toolkits from foreign countries exposes the telecommunications infrastructure to potential espionage and interference. Malicious actors may infiltrate the supply chain by installing malicious hardware components or software backdoors in telecommunications equipment. Employees or contractors can be recruited or coerced to provide access to networks and systems. Outsourcing firmware development to third-party suppliers means a lack of direct oversight and varying cybersecurity practices among suppliers.</p>

Threat	Evidence
Global market demands	<p>The global nature of the telecommunications supply chain makes it challenging to maintain security standards across all components and partners; each link in the chain may have different levels of security maturity.</p> <p>Australia is often behind other countries in the queue for new spectrum allocations. Falling behind in spectrum allocation can affect the country's ability to deploy the latest wireless technologies, such as 5G and future 6G networks, in a timely manner. This delay can be due to slower regulatory processes, political considerations, or less aggressive bidding strategies compared to other nations.</p> <p>The lack of a domestic ecosystem in telecommunications manufacturing means that Australia, like other countries, relies on a few suppliers. The characteristics and potential of 5G mean it is likely to play a significant role in critical national infrastructure, going forward. The US Government has been advocating for a 'clean network', demonstrating increased momentum to diversify supply chains away from particular markets, such as China.¹²²</p> <p>Supply chain disruption has driven some innovation towards integrating circular economy into business strategy to maintain the momentum of planned rollouts through the repurposing of equipment.¹²³</p> <p>Australia, Canada, the United Kingdom, and the United States released a joint statement on Telecommunications Supplier Diversity, which committed "to ensuring the security and resilience of our telecommunications networks, including by fostering a diverse supply chain and influencing the development of future telecommunications technologies such as 6G."¹²⁴</p>

122 United States Department of State 2021, *The Clean Network - United States Department of State*, <https://2017-2021.state.gov/the-clean-network/>

123 Amir, S, Salehi, N, Roci, M, Sweet, S & Rashid, A 2022, 'Towards Circular Economy: A Guiding Framework for Circular Supply Chain Implementation', *Business Strategy and the Environment*, vol. 32, no. 6, <https://doi.org/10.1002/bse.3264>

124 National Telecommunications and Information Administration, The Department of Home Affairs, The Department of Innovation, Science and Economic Development Canada & The Department for Digital, Culture, Media and Sport 2022, *Joint Statement Between the United States of America, Australia, Canada and the United Kingdom on Telecommunications Supplier Diversity*, National Telecommunications and Information Administration, <https://www.ntia.gov/press-release/2022/joint-statement-between-united-states-america-australia-canada-and-united>

Gaps

The below threat was not identified by project stakeholders or was only briefly acknowledged, despite broader literature indicating their importance to situational awareness of the current risk horizon:

- delayed development of a national capability.

Table 17. Gaps in supply chain threats identified by the project team

Threat	Description
Delayed development of a national capability	<p>One supply chain threat stakeholders overlooked was the delayed development of national capability in Australia's telecommunications sector. Despite advocacy for bolstering domestic capabilities, initiatives like the Prague Proposals on Telecommunications Supplier Diversity¹²⁵ and the Open RAN Principles¹²⁶ have not received adequate support. Additionally, a lack of innovation and funding hinders progress in this area, particularly the development of cases for 5G and their connection to the economic growth of other sectors.</p> <p>Delays may stem from sluggish industry policy processes, a poor history of manufacturing and research and development, political factors, or less competitive markets compared to other nations.</p>

¹²⁵ Prague Proposals 2021, Explore Key Takeaways from Prague Proposal, <https://www.praguecybersecurityconference.com/prague-proposals/>

¹²⁶ Department for Digital, Culture, Media & Sport and Department for Science, Innovation & Technology 2022, *Open RAN Principles*, GOV.UK, <https://www.gov.uk/government/publications/uk-open-ran-principles/open-ran-principles>

Threat sources: Who or what initiates disruption?

A threat requires an initiating source to become active. Identifying the threat source allows for greater precision in discussing threats to, and therefore resilience of, the telecommunications sector. Understanding what makes a threat move from passive to active helps to clarify what factor of risk needs to be considered for mitigation. Intent of action, including motivation or capability, can influence the likelihood of a threat source acting on a vulnerability to create a disruptive event.¹²⁷

The section that follows profiles malicious and non-malicious threats identified by project stakeholders.

Malicious threat sources

Malicious threat sources refer to entities or agents with the motivation and capability to initiate threats for the purpose of causing harm, disruption, or damage to systems, organisations, or infrastructure. These actions are intentional and often aim to exploit vulnerabilities to compromise the confidentiality, integrity, or availability of data or information. Malicious threat sources can take various forms, including individuals, groups, organisations, or foreign states, each employing a range of methods and techniques to achieve their harmful objectives.

Table 18. Malicious threat sources identified by stakeholders

Malicious threat source	Description
Individuals	Skilled hackers or insiders who target network vulnerabilities to compromise data confidentiality, integrity, or availability. Vandals may also target physical infrastructure to cause damage.
Cybercriminal groups	Cybercriminal groups that launch coordinated attacks aimed at disrupting essential services, leading to widespread outages.
Organisations	Entities engaging in corporate espionage to steal sensitive information, impacting the security of telecommunications networks.
Foreign states	State-sponsored actors conducting cyber operations to compromise national telecommunications infrastructure, threatening security and sovereignty.

¹²⁷ Ibid.

Non-malicious threat sources

Non-malicious threat sources encompass a spectrum of unintentional and naturally occurring factors that could potentially initiate a threat. These sources lack malicious intent and include instances of human error, neglect, accidents, natural phenomena, and the unplanned impact of emerging technologies. These threats can lead to disruptions in telecommunications infrastructure and services without the intent to cause harm.

Table 19. Non-malicious threat sources identified by stakeholders

Non-malicious threat source	Description
Human error	Unintentional mistakes in the configuration or maintenance of telecommunications infrastructure, leading to service disruption.
Accidental damage	Damage caused by construction activities or other unforeseen events that can disrupt telecommunications services.
Natural phenomena	Environmental or climactic events such as bushfires, severe weather, or floods that threaten the stability and functionality of telecommunications infrastructure.
Emerging technologies	The introduction of new technologies that may unintentionally cause disruption if not properly planned, configured, or integrated with existing systems.

Vulnerabilities: What makes the sector vulnerable to disruption?

“Addressing vulnerabilities is a Sisyphean challenge that must be sustained.”¹²⁸

For disruption to occur, a threat and a vulnerability must exist and become active. Vulnerabilities are inevitable, and not all vulnerabilities can be identified, removed, or minimised.

- There are threats and vulnerabilities that remain passive and don't become a disruption.
- There are threats and vulnerabilities that become a disruption that degrade the system, but the system can still perform.
- There are active threats and vulnerabilities that are disruptive, meaning that they are catastrophic, severely or totally disrupting the system's performance.

TPDC vulnerability categories

Vulnerabilities are traditionally classified according to the asset class they relate to: hardware, software, network, personnel, physical, and organisational factors.¹²⁹ However, Barnes posits that for critical assets, services and systems, vulnerabilities can be simplified to three vulnerability-creating elements: human, virtual; or physical (see Table 20).

For the purposes of this project, TPDC has adopted the simplified vulnerability-creating categories based on Barnes' work,¹³⁰ with the understanding that these are determined by physical, social, economic, and environmental factors that contribute to sector disruption.

Table 20. Mapping vulnerability categories

Vulnerability creating categories (Barnes)	Asset class (ISO/IEC 27005:2022)
Human	Personnel, organisational
Virtual	Software, network
Physical	Hardware, physical

The following analysis reveals patterns of vulnerability across these human, virtual and physical categories.

128 Risk and Resilience Expert Panellist, 2024.
129 International Organization for Standardization 2015, 15288-2023 - ISO/IEC/IEEE International Standard - Systems and software engineering-- System life cycle processes, <https://ieeexplore.ieee.org/document/10123367>
130 Barnes, P 2016, Training Material at the Australian Strategic Policy Institute, Australian Strategic Policy Institute, Canberra.

Vulnerabilities created by humans

How do humans create vulnerabilities?

Decisions and choices by human actors can result in inbuilt vulnerabilities as well as inbuilt strengths.¹³¹ Human vulnerabilities in the telecommunications sector are linked to human-driven decision-making, responsibility, and values within both commercial enterprises and governments.¹³²

What does this mean for sector resilience?

Weaknesses within enterprises directly influence levels of vulnerability within the sector and, moreover, the sector's ability to be resilient against disruption.¹³³

Recognising that humans contribute to vulnerabilities through decision-making, behaviour, and oversight highlights the importance of training, awareness, and responsible practices as a means by which to mitigate human vulnerabilities.¹³⁴

In Australia, the approach that incentivises cohesion of commercial imperatives and sector outcomes in critical infrastructure sectors is known as organisational resilience. For example, the Department of Home Affairs Cyber and Infrastructure Security Centre (CISC) has developed an Organisational Resilience Good Practice Guide for enterprises that sets out a framework for maturing resilience at the organisational level.¹³⁵

The Organisational Resilience Good Practice Guide identifies 13 behavioural indicators: leadership, decision-making, situational awareness, creativity and innovation, employee engagement, collaboration, resource management, knowledge management, silo mentality, exercise management, foresight, unity of purpose, and proactive posture.¹³⁶

What human-created vulnerabilities did project stakeholders identify?

The evidence table below shows recurring patterns related to failure to integrate lessons from disruption. The case has not been built at a whole-of-nation level to cement cohesion between commercial imperatives and sector outcomes. Ongoing cost pressures and technological changes have led to reduced labour force across the sector. This has created a strong perception that the sector lacks the necessary skills, and those available are not aligned with where they are needed most.

Weak lesson management across the sector means that lessons from past events have not driven significant change. This is evidence that the lack of a structured national approach to climate risk assessment in infrastructure planning has left the sector ill-prepared for climate-related disruptions. Hence, there are doubts across the sector about the capacity to handle unprecedented situations.

131 National Resilience Taskforce 2018, *Profiling Australia's Vulnerability: interconnected causes and cascading effects of systemic disaster risk*, Australian Institute for Disaster Resilience, <https://www.aidr.org.au/media/6682/national-resilience-taskforce-profiling-australias-vulnerability.pdf>

132 International Organization for Standardization 2017, *ISO 22316:2017 Security and resilience — Organizational resilience — Principles and attributes*, <https://www.iso.org/standard/50053.html>

133 Pescaroli, G & Alexander, D 2018, 'Understanding Compound, Interconnected, Interacting, and Cascading Risks: A Holistic Framework', *Risk Analysis* vol. 38, <https://doi.org/10.1111/risa.13128>

134 International Organization for Standardization 2017, *ISO 22316:2017 Security and resilience — Organizational resilience — Principles and attributes*, <https://www.iso.org/standard/50053.html>

135 Department of Home Affairs 2024, *Organisational Resilience: Good Practice Guide*, <https://www.cisc.gov.au/how-we-support-industry-subsite/Documents/org-res-good-practice-guide.pdf>

136 Ibid.

Table 21. Human-created vulnerabilities identified by stakeholders

Vulnerability	Evidence
Failure to effectively learn lessons from disruption	The sector has had little pause in disruption over the past five years, meaning that there is a sense of continually reacting to events, rather than adopting proactive measures. There is still a tension between accepting that this cadence of disruption will likely be ongoing, and expecting that there will be a lull that enables regrouping and forward planning.
Fragmented accountability	Private ownership of critical infrastructure fragments accountability and coordination efforts, hindering comprehensive sector-wide preparedness and response strategies. Efforts to align commercial imperatives with sector outcomes have not been effectively implemented in practice.
Weak information sharing	Lack of information and data-sharing practices, compounded by weak internal cultures and crisis communication within organisations, impedes effective incident escalation during outages or security breaches.
Siloed practices	Security and information sharing between commercial competitors are not recognised as a competitive advantage, leading to siloed practices and insufficient collective defence mechanisms.
Skill shortages	Australia lacks sufficient telecommunications engineers and technical specialists to handle legacy infrastructure and emerging technologies. The shortage of skilled workers and funded agencies limits efforts to build capability across disruption management phases.
Geographic skill disparities	Expertise needed for cyber incidents often resides in global operations centres rather than onshore. Network architecture, cyber response, and call-centre functions rely on offshore staff, and labour market dynamics contribute to a scarcity of skilled personnel for infrastructure rebuilding.
Climate risk integration	Absence of standardised climate risk assessments and methodologies for mapping environmental threats specific to the telecommunications sector. The lack of a structured national approach leads to uncertainties and insufficient proactive measures for climate-related issues.
Learning from past events	Events like a catastrophic bushfire, cyberattack, capacity issues during a pandemic, or errors in software updates understandably prompt preparedness activities to address vulnerabilities. These events within a particular jurisdiction tend to shape subsequent strategies concerning resilience, regulation, and the public sector's role in enhancing it. The challenge is that efforts to learn (e.g. Royal Commission into National Natural Disaster Arrangements) have not actually driven widespread systemic resilience. Dependency between the energy sector and communications remains little understood, and worse, mechanisms to enhance it, such as a Memorandum of Understanding to enhance information sharing between the sectors, recommended by the Royal Commission, have not driven change (see Physical, and Environmental and Climate Threats).

Vulnerability	Evidence
Supply chains	<p>Reliance on foreign components, software, and toolkits is viewed as a long-term vulnerability. Telecommunications carriers may need to avoid equipment or services from foreign companies, subject to extra-judicial directives, especially concerning 5G technology.</p> <p>Global vendors demonstrated the robustness of their supply chain over the pandemic. Risk assessments are needed to consider the mitigation plans of foreign-owned companies that are key suppliers to the Australian market. Mobile network operators undertake their own risk assessment when selecting vendors, which includes supply chain security assessments. However, risk assessments should cover all key suppliers.</p>
Market structure	<p>The presence of monopolies such as the NBN wholesale monopoly and oligopolies dominated by Telstra, Optus, and TPG, concentrates control within a limited number of entities. Small and medium-sized enterprises (SMEs) face inherent resource constraints compared to larger enterprises, limiting their ability to invest in robust cybersecurity measures and resilience-building initiatives.</p>
Allocation of investment	<p>Investment funds are often directed towards specific entities rather than place-based improvements, resulting in insufficient incentives to enhance resilience at the local level. The reliance on grant programs with co-contributions from telcos and the government raises concerns about public funding for for-profit entities.</p>
Sectoral engagement	<p>The National Coordination Mechanism (NCM) is underutilised, and there is a need for better engagement between all levels of government and industry to determine priorities for action that address incident consequences and broader management.</p>
Lack of incentives	<p>Without the right incentives, processes or procedures for individual enterprises to share vulnerability intelligence at the sector-level, the sector is more susceptible to having vulnerabilities exploited.</p>

Vulnerabilities created by virtual elements

How do virtual elements create vulnerabilities?

Virtual vulnerabilities in the telecommunications sector are linked to systems and networks within the telecommunications sector, including telephony, wireless communications, data storage structures, and cloud systems.

In telephony, outdated encryption protocols or insecure call routing practices may create network vulnerabilities, potentially exposing communications to interception or manipulation. In wireless communications systems, unauthorised access points or insufficient encryption measures may increase the likelihood of exposure to data breaches or service disruptions.

In internet networks, widespread network vulnerabilities occur due to route hijacking, through malicious or non-malicious actors. The widespread failure of many Australian entities to adopt route resilience mechanisms through proper route authorisation and validation (RPKI) means the sector maintains a high level of vulnerability.

What does this mean for sector resilience?

Inadequate data storage infrastructure and security may be susceptible to cyber threats such as ransomware, leading to compromised information integrity and availability. Additionally, reliance on dynamic cloud systems may, for example, introduce misconfigurations, amplifying the impact of cyber incidents across the network.

How virtual vulnerabilities are identified within an enterprise and how they are reported or shared at the sector-level is important for sector resilience.

What virtually created vulnerabilities did project stakeholders identify?

The evidence tabled below indicates recurring patterns related to the failure to integrate lessons from disruption. Threat detection is a predominant focus within current research paradigms, but with a growing interest in the need to focus on network recovery, and the development of industry playbooks to guide consequence management capabilities.

There is a widespread reluctance to share information about vulnerabilities due to fear of regulatory repercussions. Some stakeholders suggested that parts of the sector over-interpreted the negative regulatory repercussions of information-sharing. Capacity shortages create operational challenges, and limited real-time monitoring and threat response capabilities leave the sector vulnerable

The expansion of cloud-based deployments and encryption practices has broadened the attack surface, increasing the potential for breaches, even as these developments increase prospects for economic activity through applications such as the IoT. As telecommunications entities continue to digitise, their data holdings become increasingly valuable, making them a more attractive target for sophisticated cyber threat actors.

Table 22. Virtually created vulnerabilities identified by stakeholders

Vulnerability	Evidence
Focus on threat detection over recovery	<p>Technically focused research aims to ensure that networks are not easily disrupted (particularly through detection and monitoring). There is less focus on the effective recovery of networks after mass national or widescale outages.¹³⁷</p> <p>This means there are unclear guides of what needs to occur in technical and policy terms for the recovery of networks in the event of a national or widescale outage. The base requirement for telecommunications operators is to 'restore to last known backup', but there is also a need to determine 'data recovery objectives' and 'time recovery objectives'.¹³⁸</p>
Lack of cooperative policy and regulation	<p>There is an absence of guidance material that builds a national picture of the interplay of telecommunications networks, resilience regulation, and government more broadly. The connection between telecommunications and the energy sector in the event of widespread outages needs strong cooperative policy and regulation to assist outcomes, including the development of shared crisis frameworks, procedures and teams.</p>
Reluctance to share vulnerability information	<p>There is a perception in the industry that sharing vulnerability intelligence might make telecommunications entities more susceptible to having those vulnerabilities exploited or expose the entity to accusations of anti-competitive conduct.</p>
Third-party providers	<p>Published inquiries identified that third-party providers have caused issues with large-scale outages, with DDoS attacks occurring due to the failure to re-configure default settings.¹³⁹ In addition, the implementation of weak contracts and project management by affected entities has affected service delivery.</p>

137 Owen R 2024, Broadband Technology Research Unit (BTRU) at University of Technology Sydney (Faculty of Engineering and Information Technology), private correspondence.

138 Kozine, I & Andersen, H 2015, *Integration of Resilience Capabilities for Critical Infrastructures Into the Emergency Management Set-up*, Safety and Reliability of Complex Engineered Systems, CRC Press, https://backend.orbit.dtu.dk/ws/files/128948305/Paper_ESREL_2015_postprint.pdf

139 *The 2016 Census (referred to as #censusfail) was hit by a distributed denial-of-service attack. The website was flooded with traffic in an attempt to overload it and shut it down. The published inquiry noted that contract management on the part of the Australian Bureau of Statistics (ABS) eCensus could have been strengthened: The ABS could have been more proactive in overseeing the implementation of the eCensus project. "They could have had more third-party testing done. They may have asked more questions of IBM to provide proof that they were delivering the services they were contracted to do."* Senate Economics Reference Committee 2017, 2016 Census: issues of trust, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/2016Census/Report

Vulnerability	Evidence
Absence of cross-carrier disaster roaming	The absence of cross-carrier disaster roaming capabilities limits the interoperability of telecommunications networks, exacerbating service disruptions and security vulnerabilities. ¹⁴⁰ A push to develop such capabilities has been met with resistance, given the technology's limitations and cost involved. ¹⁴¹
Capacity shortages	Network congestion due to capacity shortages in spectrum, backhaul and access infrastructure poses operational challenges during peak demand periods, including during outages.
Limited real-time monitoring	The lack of real-time monitoring and data accessibility hampers proactive threat detection and response, leaving networks vulnerable to evolving cyber threats.
Expanding attack surface	Cloud-based deployments and open 5G RAN architectures significantly expand the attack surface for cyber threats. Limited awareness of emerging threats, such as false base stations (FBS) and SIM swaps, coupled with inadequate detection capabilities, makes telecommunications networks attractive targets for malicious actors. ¹⁴²
Cybersecurity weaknesses	<p>Cybersecurity vulnerabilities within the telecommunications sector include insecure call routing practices, outdated encryption protocols, and dependencies on dynamic cloud systems that can lead to misconfigurations. The sector's reliance on equipment designed for specific spectrum bands also presents compatibility issues, as spectrum re-allocation may render existing hardware incompatible.</p> <p>Insufficient encryption measures in wireless communications and the persistence of outdated encryption protocols in telephony pose significant security challenges, potentially exposing sensitive data to interception and exploitation. International supply chain dependencies, especially in configuration and software, introduce security challenges due to potential foreign influence.</p> <p>The lack of adoption of route origin authorisation and validation in Australia's major networks is of serious concern.</p>
International supply chain dependencies	Dependencies on international supply chains, especially in configuration and software, introduce security challenges due to potential foreign influence.
Data monetisation	<p>Due to declining profits, Telecommunications providers face strong commercial imperatives to monetise their data assets.</p> <p>The vast data holdings of telecommunications providers present lucrative targets for cyber-attacks. Anonymised data is rarely ever completely un-hackable, as it can often be reassembled to reveal the original information.¹⁴³ A shared, sector-wide approach can fortify the sector against vulnerabilities and bolster consequence management capabilities, ensuring a more robust defence against potential breaches.</p>

140 Australian Competition and Consumer Commission 2023, *Regional Mobile Infrastructure Inquiry*, <https://www.accc.gov.au/system/files/Regional%20Mobile%20Infrastructure%20Inquiry%20final%20report.pdf>

141 Senate Select Committee on Australia's Disaster Resilience 2023, *Interim Report*, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Disaster_Resilience/DisasterResilience/Interim_Report

142 Ottosson, M 2022, *Why network intelligence is vital in addressing RAN threats*, Ericsson, <https://www.ericsson.com/en/blog/2022/6/why-network-intelligence-is-vital-in-addressing-ran-threats>

143 Rocher, L, Hendrickx, J & Montjoye, Y 2019, 'Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models', *Nature Communications*, vol. 10, <https://doi.org/10.1038/s41467-019-10933-3>

Vulnerabilities created by physical elements

How do physical elements create vulnerabilities?

Physical vulnerabilities in the telecommunications sector are linked to physical parts of the system, including the physical elements of the information and communication technology (ICT) environment, built infrastructure, and landscape considerations. Vulnerabilities can arise from physical elements of ICT infrastructure and components, including servers, data storage systems, and communication hardware.

Built infrastructure, such as network facilities and equipment, represents another focal point where weaknesses may expose the sector to disruption. Additionally, landscape considerations encompass evaluating environmental and geographical factors, including the strategic placement of critical infrastructure in regions susceptible to environmental threats like bushfires, floods, or other environmental disturbances.

What does this mean for sectoral resilience?

Failing to conduct thorough strategic planning and assess the physical landscape's impact on telecommunication infrastructure can create vulnerability, leading to a higher likelihood of exposure to disruption.

What physically created vulnerabilities did project stakeholders identify?

The evidence tabled below shows recurring patterns related to failure to integrate lessons from disruption. Despite efforts to manage energy interdependency through a Memorandum of Understanding (MoU)¹⁴⁴ between the sectors, this has not led to needed cooperation or coordination.

Legacy infrastructure remains vulnerable to faults and is challenging to service due to difficulties in sourcing spare parts. There is a widespread perception that single points of failure across the network make the sector susceptible to significant disruptions. Additionally, community preparedness and place-based solutions are often neglected, leaving local areas less equipped to manage telecommunications disruptions. Designing solutions appropriate for the scale needed is weakly integrated.

Table 23. Physically-created vulnerabilities identified by stakeholders

Vulnerability	Evidence
Single points of failure	<p>In many remote, rural, and regional areas (RRR) of Australia, critical communication networks rely on singular or few main-line fibre optic cables, with limited backup or redundancy measures in place. There has been a historical underinvestment in RRR infrastructure and a lack of diversification in infrastructure, networks, and service providers.</p> <p>Sub-sea cables, which are essential for international connectivity, represent another potential single point of failure due to their limited number and susceptibility to damage from natural disasters or human activities, including accidents and intentional damage.</p>

¹⁴⁴ Energy Networks Australia 2020, *Memorandum of Understanding (MoU) between Energy Networks Australia and Communications Alliance*, <https://www.energynetworks.com.au/news/ena-and-comms-alliance-mou/>

Vulnerability	Evidence
Energy interdependency and coordination	<p>There is a lack of coordination, information-sharing, and awareness regarding critical interdependencies between energy sources and telecommunications infrastructure. Efforts towards sustainability and decarbonisation, which often involve transitioning to alternative energy sources, have not occurred.</p> <p>The energy interdependencies within the telecommunications sector also contribute to physical vulnerabilities. The technical feasibility of implementing redundancy measures in energy supply systems remains a challenge, potentially leaving critical infrastructure vulnerable to prolonged disruptions.</p>
Legacy infrastructure	<p>The aging copper network is increasingly susceptible to faults and disruptions, including theft. The vast geography of Australia presents a practical challenge, with thousands of square kilometres lacking adequate connectivity due to the sheer size and remoteness of these locations. Many sites in these remote areas are physically inaccessible, further complicating efforts to maintain and repair infrastructure.</p>
Lack of community preparedness and place-based solutions	<p>The lack of community preparedness contributes to physical vulnerabilities, particularly in rural and remote areas heavily reliant on mobile networks. The absence of place-based solutions and redundancy measures leaves these communities vulnerable to prolonged service disruptions during emergencies or network failures. Additionally, certain rural and remote regions still lack access to even the previous generation of mobile network technology, such as 4G, highlighting disparities in telecommunications infrastructure across the country.</p>
Dependence of foreign components and services	<p>Many telecommunications providers in Australia heavily rely on components, software, and toolkits sourced from foreign countries, which can introduce security risks related to extra-judicial directives and geopolitical influences. For instance, critical emergency services, such as police vehicles, rely on services provided by foreign corporations like Starlink's LEOSat, raising concerns about sovereignty and dependence on external entities for essential infrastructure services.</p>

Step 3: Adapt, respond, recover: Building consequence management capabilities

TPDC definition of consequence management

Consequence management is the conceptual and operational approach to 'lessening the effects' of a disruption (i.e. reducing its magnitude and the trajectory of its impact(s)) and is underpinned by the development of capabilities. Consequence management is distinct from and broader than emergency management or cyber incident management.¹⁴⁵ "Emergency management" deals with a particular incident; while "consequence management" understands the broader consequences of a disruption, to mitigate its total impact.¹⁴⁶

At the sector-level, consequence management requires maturing capacities and building capabilities within the enabling environment through regulation, coordination, cooperation and collective action.

Consequence management prepares entities to effectively adapt, respond, and recover when disruptions occur, with the aim of ensuring business and service continuity, safeguarding stakeholders, and maintaining public trust.

The goal of consequence management is to ensure that response and recovery efforts "deliver positive outcomes [and] that action – or inaction – does not exacerbate adverse consequences" and does so within resource constraints.¹⁴⁷ Consequence management may also play a potential contribution to the deterrence of disruptive events (at least those that are human-induced).¹⁴⁸

For adaptive response and recovery capacities to mature at the sector-level, consequence management capabilities need to be built across all entities and stakeholders.

Consequence management and its importance to risk management and lessons management risk management aims to detect and prevent disruption. Once a disruptive event occurs, there is no longer any real meaning for risk, and its probabilistic nature.¹⁴⁹ The probable has become actual. Necessarily, the focus shifts to consequence management. Performance needs to recover and be sustained when disruptions occur. Consequence management is the means to achieve this.

145 Durkovich, C 2020, *Protecting Critical Infrastructure*, The MIT Press eBooks, <https://doi.org/10.7551/mitpress/13831.003.0012>

146 Ibid.

147 Ibid.

148 Kartchner, K 2013, *Consequence Management and National Security*, US eBooks, https://doi.org/10.1057/9781137336439_13 Department of Defence 2022, *National Defence: Defence Strategic Review*, <https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review>

149 Branagan, M 2012, 'A Risk Simulation Framework for Information Infrastructure Protection' PhD thesis, Queensland University of Technology, https://eprints.qut.edu.au/51006/1/Mark_Branagan_Thesis.pdf

Implications of consequence management for risk management

The outcomes and lessons from consequence management efforts during and after disruptions can provide valuable insights to inform and enhance risk management. By analysing the effectiveness of response and recovery strategies, as well as the impacts and cascading effects, the sector can refine risk assessment and prioritisation.

The feedback loop enables the identification of previously unrecognised vulnerabilities, interdependencies and unforeseen impacts.

Implications of consequence management for lessons management

Effective consequence management during disruptions not only mitigates immediate impacts, but also presents invaluable opportunities for learning and improvement. By closely monitoring and evaluating the outcomes of response and recovery efforts, valuable lessons can be learned regarding the effectiveness of existing plans, procedures, and capabilities.

When systematically captured and analysed, these lessons can inform the refinement of consequence management strategies, enabling the sector to continuously enhance its ability to respond to and recover from future disruptions.

Elements of good consequence management

Good consequence management in the telecommunications sector involves a proactive and strategic approach to preparing for, responding to, and recovering from disruptions. It involves:

- preparing for disruption from an all-hazards perspective¹⁵⁰
- thinking about telecommunications infrastructure in its broader systemic context, including linkages with energy, transportation, and financial infrastructures¹⁵¹
- considering society's dependence on telecommunications infrastructure, including where disruption leads to adverse impacts on other sectors¹⁵²
- collaborating with purpose across the sector's multiple layers and jurisdictions, and with interdependent and dependent sectors, including by creating partnerships
- building solutions beyond the immediate term by taking a lifecycle approach.

The sections that follow profile project stakeholders' views on the current weaknesses in consequence management across the telecommunications section as at June 2024. Addressing these weaknesses would significantly enhance resilience in the telecommunications sector.

150 Ward, P, Daniell, J, Duncan, M, Dunne, A, Hananel, C, Hochrainer-Stigler, S & Tijssen, A 2022, *Invited Perspectives: A Research Agenda Towards Disaster Risk Management Pathways in Multi-(Hazard-)Risk Assessment*, Natural Hazards and Earth System Sciences, vol. 22, <https://doi.org/10.5194/nhess-22-1487-2022> Department of the Prime Minister and Cabinet 2022, Australian Government Crisis Management Framework, <https://www.pmc.gov.au/sites/default/files/resource/download/australian-government-crisis-management-framework.pdf> Queensland Disaster Management 2023, *Prevention Preparedness Response and Recovery Disaster Management Guideline*, <https://www.disaster.qld.gov.au/disaster-management-guideline>

151 Kyriakides, Ed & Polycarpou, M 2015, *Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems*, Studies in Computational Intelligence, <https://doi.org/10.1007/978-3-662-44160-2>

152 Svegrup, L, Johansson, J & Hassel, H 2019, *Integration of Critical Infrastructure and Societal Consequence Models: Impact on Swedish Power System Mitigation Decisions*, Risk Analysis, vol. 39, <https://doi.org/10.1111/risa.13272>

Table 24. Capture of evidence relevant to current weaknesses in consequence management

Level	Weaknesses in current state of consequence management as identified by project stakeholders
All sector	<p>There are weaknesses in communicating crisis information to the public.</p> <p>Information is not communicated to the public in a timely, accurate, effective or useful way.</p> <p>There is a lack of availability of a national common operating picture and the expansion of a COP for jurisdictions and industry to guide consequence management and strategic planning.</p> <p>While project stakeholders acknowledged the importance of understanding risk from an all-hazards perspective, there is a mixed understanding of what 'all-hazards' means.</p> <p>There are challenges in achieving a comprehensive understanding of threats, threat sources, vulnerabilities, and consequences due to data limitations and discrepancies in expectations between government and telecommunications enterprises.</p> <p>The root cause of disruption can often be mischaracterised. For example, there can be a lot of attention on offensive cyber incidents by government, and less attention on mundane causes, such as software misconfiguration. This can lead to inefficiently allocated resources, and makes it difficult for the sector to learn from the incident and prepare for similar future disruptions.</p> <p>There is recognition of the need for a systems-level approach to telecommunications resilience, but the current state lacks a cohesive national framework, resulting in fragmented approaches to consequence management between industry and government, and between levels of government.</p> <p>There are missed opportunities to strengthen end-users reliant on telecommunications (including communities via place-based solutions or interdependent sectors). Resources are often diverted to repeating legacy solutions, rather than learning lessons and innovating.</p> <p>There is no clear definition of the 'whole of sector'.</p> <p>There is reluctance to share information because of commercial-in-confidence considerations, plus a culture of not sharing for fear of being accused of anti-competitive behaviour.</p> <p>There is a lack of scenario planning at the sector-level for surprise-events.</p> <p>There is a lack of alignment between local, state and territory and federal governmental priorities.</p> <p>Coordination across the telecommunications sector is fragmented, with inconsistencies in reporting mechanisms, data-sharing protocols, and coordination forums.</p> <p>Stakeholders, such as state and territory governments, small and medium enterprises, and communities are underrepresented in existing coordination mechanisms.</p> <p>Resources are expended, devising solutions that often lack a clear purpose or are disconnected from the operational circumstances that can improve response and recovery.</p>

Level	Weaknesses in current state of consequence management as identified by project stakeholders
Asset level information	<p>Existing national-level resources (e.g. Home Affairs Register of Assets, National Joint Common Operating Picture (NJCOP)) are currently limited in their impact, as their purpose and usage are poorly articulated.</p> <p>Approaches to threats that emphasise actors rather than assets may overlook the critical importance of safeguarding "the data crown jewels."</p> <p>Capabilities that ensure the availability and granular visibility of parts of the system, including infrastructure, people and assets (maritime and land-maintenance) and overall situational awareness in real-time are weak.</p> <p>Software supply contributes to the introduction of latent problems. The ongoing debate on sovereign capability and offshoring directly impacts software logistics, which is increasingly important as networks become software-defined and automated.</p> <p>There is a lack of integration and imagination in using existing resources, like 'Before You Dig', to build a complete picture of asset locations, including collaboration with utility providers.</p>
Bi-directional information sharing	<p>Industry shares information with the government in inconsistent formats, rendering it, at times, useless.</p> <p>There is little or no feedback from government to industry when information is shared.</p> <p>There is a perception that the government misunderstands what the sector needs.</p> <p>Over-reporting of incidents to government can create white noise, overwhelming the ability of operators to communicate in a timely, accurate, effective, or useful way.</p> <p>There is a disconnection in perspectives between government and industry regarding outages. The industry's perspective is that its priority is to return to business as usual as quickly as possible. They want help sharing real-time information for response and recovery across all sectors, and claim that the government prevents this. The perspective from the industry is that the government seeks compliance with regulation (which prevents the ability to formulate real-time information sharing).</p>
Communication Sector Group	<p>The design of the Communications Sector Group (CSG) and who is included in the CSG, limits its effectiveness as an information-sharing forum.</p> <p>Governance, including the Chair's independence, affects the group's capability.</p> <p>The role of an Australian Government department as a secretariat can limit the information that is shared.</p> <p>Small and medium firms are inconsistently engaged, and hundreds of suppliers have little idea or awareness of how their services might be improved or affected.</p>

Level	Weaknesses in current state of consequence management as identified by project stakeholders
Federal	<p>Focus on legal regulatory approaches has narrowed what industry shares with government, including threat intelligence, which is pushed to legal compliance teams before dissemination.</p> <p>Legislation to encourage competition has a chilling effect on information sharing in the sector; this is engrained in the industry's culture.</p> <p>There remains a perception gap about the role of the Australian Cyber Security Centre in the ecosystem and the advice it can provide.</p> <p>There is a lack of understanding of reporting to ACSC, such as who must report and when. In some cases, organisations choose not to share for no other reason than commercial sensitivity, even though it is creating consequences for the sector.</p> <p>There is a lack of clear guidance about layers of regulation (e.g. when incidents fall under the SOCI Act).</p> <p>It was reported that a telecommunications entity had to report to 28 areas of government after a data breach.</p> <p>There is no government mandate to prioritise traffic or pathways in the event of an incident.</p>
Interdependent and dependent sectors	<p>While there is an acknowledgement of complex interdependencies (such as the centrality of the telecommunications sector to other critical infrastructure sectors and essential services, the reliance on the energy sector, or interdependencies arising via international supply chains), these interdependencies remain poorly understood within the emergency management environment, and solutions to enhance them are not systematic. The lack of understanding plays out in emergency responses, where much time is spent explaining consequences and interdependencies to those agencies responsible for coordinating response.</p> <p>There is a lack of a comprehensive mapping of interdependencies, as well as forums for cross-sector collaboration and information-sharing.</p> <p>The telecommunications sector faces challenges in effectively preparing for and managing consequences that cascade within and across multiple sectors or consequences that compound due to interdependencies.</p>
Lifecycle of disruption	<p>Preparation for disruption in the telecommunications sector tends to be reactive rather than proactive, with a focus on immediate response rather than long-term resilience planning.</p> <p>Incorporating redundancy and robustness in the design of network infrastructure is complicated. To deal with a changing environment (e.g. more extreme weather), measures need to consider what is commercially viable or acceptable, which may not meet the expectations of communities or emergency management, which have a low tolerance for disruption.</p> <p>Business continuity and maintenance do not necessarily account for both legacy infrastructures and technological advancements.</p>

Level	Weaknesses in current state of consequence management as identified by project stakeholders
Local	<p>Tension exists between national-level information consolidation and local (place-based) solutions during crises.³⁸</p> <p>Solutions often tend to scale up rather than scaffold down to local levels.</p> <p>State-level resilience frameworks promote place-based approaches, but carriers and providers are not developing this as a capability.</p> <p>Place-based approaches to community information require terrestrial backups, not mobile or satellite solutions.</p> <p>National Coordination Mechanism</p> <p>There is a lack of clear guidance within the government over when to escalate an incident from an enterprise level to the National Coordination Mechanism.</p> <p>The purpose and outcome of activating the National Coordination Mechanism (NCM) was unclear to project stakeholders.</p> <p>The NCM is very sharp and action-focused, but the telecommunications sector has hesitated to engage with the NCM.</p> <p>Telecommunications is not designated as an essential service by state and territory emergency management frameworks (except in NSW).</p>
Provider	<p>There is a time factor that limits effective information sharing, including knowledge of the level at which issues emerge (e.g. modems, devices).</p> <p>There is an assumption that enterprise-level responses (incident management and crisis management) are fit for purpose.</p> <p>The reputation of telecommunications and consumer perceptions may lead to incidents being escalated prematurely or, conversely, kept in-house when external action is necessary.</p> <p>There is a lack of understanding of which services should be prioritised for restoration in the event of failure.</p>
Public-Private cooperation	<p>To some extent, public-private cooperation and partnerships exist to some extent but are limited by challenges such as commercial concerns and mismatched expectations.</p> <p>The concept of public-private partnership is limited to incumbents rather than including other stakeholders, such as local councils, emergency service operators, entrepreneurs, and community groups.</p> <p>Competition policy is producing unintended consequences, such as creating a handout mentality.</p> <p>There is weak collaboration between government and industry stakeholders; thus, a shared vision for telecommunications resilience has not been developed.</p>

Level	Weaknesses in current state of consequence management as identified by project stakeholders
Service level	<p>There is a mismatch between the expectations of end-users (customers) and telecommunications providers' service level objectives (SLOs). There are specific goals set by providers regarding the quality and performance of the service, including uptime guarantees, response times, and data throughput rates. End-users might not fully understand the actual service levels they are entitled, leading to a misconception about the service quality they should expect. Telecommunications providers may not transparently communicate their SLOs meaning that end-users cannot gauge whether the service meets their needs or if the provider is meeting their contractual obligation.</p> <p>Telecommunications providers' operational assurance systems do not convincingly demonstrate their capability to meet promised service levels as outlined in service level agreements (SLAs).¹⁵³</p> <p>Telecommunications providers do not have standardised benchmarks or accepted criteria for service levels. Providers may each have their own definitions and benchmarks for service quality, performance and reliability.</p> <p>In the event of failure, there are no standardised expectations or benchmarks for how quickly telecommunications providers should restore services after a failure or outage (such as recovery-time objectives).¹⁵⁴</p>
States and Territory	<p>Telecommunications providers have to negotiate between multiple states and territories on data sharing.</p> <p>There are different institutional capabilities across the states and territories. Lessons and technological innovations are not shared across jurisdictions.</p> <p>At the state level, there is an assumption that, at the state level, there is a low maturity in thinking on issues facing the sector (including cyber security), as communications sit in the Commonwealth domain.</p>
University sector	<p>The network between universities (AARNet) is under-utilised.</p>

¹⁵³ SLAs are crucial for setting customer expectations and providing a basis for accountability. Operational Assurance Systems include the tools protocols used by providers to ensure their services meet predefined performance and reliability standards, and include network monitoring tools, automated alerts, performance analytics and incident response mechanisms.

¹⁵⁴ Recovery-time objectives (RTOs) are specific goals set by service providers for the maximum acceptable amount of time that systems, applications or functions can be offline before an incident before negatively affecting a business or customers. RTOs are critical for planning and managing recovery efforts.

Step 4: Learn and transform: lessons management

TPDC definition of lessons management

Lessons management is an integrated principled approach to capturing, analysing and applying lessons learned from past experiences to improve future performance.

Resilience is not a static characteristic but rather a continuous, iterative process of learning and transformation.¹⁵⁵

Adopting a principled approach to lessons management improves the sector's capacity to manage disruptions. Mature lessons management and consequence management sharpen the sector's capacity to manage the dynamic risk horizon.

The preceding sections provide a comprehensive profile of risk factors: threats, threat sources, vulnerabilities, and consequence management within the Australian telecommunications sector. Fostering sector resilience requires harnessing this evidence and linking the phases of disruption management: preparation, absorption, adaptation, response, recovery, and transformation, through robust lessons management practices.

In the context of the Australian telecommunications sector, lessons management involves systematically gathering insights to mature resilience capacities and build capabilities at the sector-level. No preexisting framework existed to model or assess lessons management across the phases of disruption.

An integral part of lessons management is change management. The sector's ability to demonstrate changed behaviour is limited unless the change can be observed across the sector, and it can be determined that the lessons were learned sector-wide, that is, the actions taken have improved the sector's resilience capacity.

To address this gap, TPDC developed the **Sector Resilience Maturity Model**.¹⁵⁶ This model, presented in Part 2 above, includes a comprehensive assessment of the maturity of the Australian telecommunications sector's resilience. This assessment leverages evidence from the preceding sections.

Repeating the application of the Profile and SRMM at regular intervals, as recommended in Section 2, will enable an iterative assessment of the sector's ability to transform its resilience maturity over time. The detailed assessments will act as a guide identifying areas where lessons need to be learned, and further work prioritised. Ongoing applications of the SRMM will help assess the extent to which sectoral lessons are being learned and applied so that sectoral resilience maturity progresses beyond the benchmark established in this initial profile.

The key point for all sector stakeholders is that by working together to systematically integrate, consistently apply, and continuously improve resilience approaches, resilience becomes greater than the sum of its parts.

Self-assessment by industry of resilience maturity is an opportunity for those enterprises to share lessons learned and guide whole-of-sector improvement. This is the value of the maturity model: it provides a shared vision and ambition of where the Australian telecommunications sector might go together.

¹⁵⁵ Mentges, A, Halekotte, L, Schneider, M, Demmer T & Lichte, D 2023, 'A Resilience Glossary Shaped by Context: Reviewing Resilience-related Terms for Critical Infrastructures', *International Journal of Disaster Risk Reduction*, vol. 96, <https://doi.org/10.1016/j.ijdrr.2023.103893>

¹⁵⁶ See Appendix B for overview of the methodology used to develop the SRMM.

Appendices

Appendix A. Glossary

Key Term	Definition
Absorb	The ability of the Australian telecommunications sector to mitigate or prevent negative impacts, using predetermined coping responses in order to preserve and restore essential assets and services to fulfil the purpose of the sector. ¹⁵⁷
Adapt	The ability of the Australian telecommunications sector to incrementally or temporarily adjust, modify or change its characteristics and actions to moderate future damage and to take advantage of opportunities so that it can continue to function without major changes to the viability of its assets or services. ¹⁵⁸
All-hazards	Accounting for all forms of human, technical and natural threats, ranging from terrorism and sabotage to technical system failures and natural disasters. ¹⁵⁹ Dealing with all types of emergencies or disasters and civil defence, using the same set of management arrangements. ¹⁶⁰
Asset	An item of value to stakeholders, which may be tangible (e.g., a physical item such as hardware, firmware, computing platform, network device, or other technology component) or intangible (e.g., humans, data, information, software, capability, function, trademark, copyright, patent, intellectual property, image, or reputation). ¹⁶¹
Asset value	The value of an asset is based on a stakeholder's assessment of the asset's role in fulfilling the overall purpose of the sector and a consequence of its loss across the entire system life-cycle. Such concerns include business, environmental, society, economy, and national security. ¹⁶²

¹⁵⁷ Organisation for Economic Development n.d., *Guidelines for Resilience Systems Analysis: How to Analyse Risk and Build a Roadmap to Resilience*, OECD iLibrary, https://www.oecd-ilibrary.org/development/guidelines-for-resilience-systems-analysis-how-to-analyse-risk-and-build-a-roadmap-to-resilience_3b1d3efe-en

¹⁵⁸ Ibid.

¹⁵⁹ Fjäder, C 2014, 'The Nation-state, National Security and Resilience in the Age of Globalisation', *Resilience* vol. 2, <https://doi.org/10.1080/21693293.2014.914771>

¹⁶⁰ Adini, B, Goldberg, A, Cohen, R, Laor, D & Bar-Dayana, Y 2012, 'Evidence-based support for the all-hazards approach to emergency preparedness', *Israel Journal of Health Policy Research*, vol. 1, no. 40, viewed 25 October 2012, <https://doi.org/10.1186/2045-4015-1-40>

¹⁶¹ Ross, R, Pillitteri, V, Graubart, R, Bodeau, B & McQuaid, R 2021, *Developing Cyber-Resilient Systems: A Systems Engineering Approach*, National Institute of Standards and Technology, <https://doi.org/10.6028/nist.sp.800-160v2r1>

¹⁶² Ibid.

Key Term	Definition
Consequence	A consequence is the result of a threat manifesting via a vulnerability. Consequence does not inherently indicate anything about risk, but rather signifies a result of an event. ¹⁶³ Consequence can vary widely, encompassing financial loss, environmental impact, loss of life, or even the occurrence of another event. ¹⁶⁴
Disruptive event	An event that prevents, or interrupts, the usual functioning of a telecommunications system or network.
Entity	An individual (person), organisation, device or process. ¹⁶⁵
Interdependency	<p>An interdependency is a bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other. Two infrastructures are physically interdependent if the state of each is dependent on the material output(s) of the other.</p> <p>An infrastructure has a cyber interdependency if its state depends on information transmitted through the information infrastructure. Infrastructures are geographically interdependent if a local environmental event can create state changes in all of them. Two infrastructures are logically interdependent if the state of each depends on the state of the other via a mechanism that is not a physical, cyber, or geographic connection.¹⁶⁶</p>
Likelihood	The probability or possibility of an event occurring. ¹⁶⁷
Magnitude of Consequence	Magnitude of consequence refers to the actual and perceived consequence means to a specific stakeholder. The magnitude of a consequence can overwhelm the probability of an event and increase the level of risk. ¹⁶⁸

¹⁶³ Branagan, M 2012, 'A Risk Simulation Framework for Information Infrastructure Protection' PhD thesis, Queensland University of Technology, https://eprints.qut.edu.au/51006/1/Mark_Branagan_Thesis.pdf

¹⁶⁴ Pescaroli, G & Alexander, D 2016, *Critical Infrastructure, Panarchies and the Vulnerability Paths of Cascading Disasters*, Natural Hazards 82, <https://doi.org/10.1007/s11069-016-2186-3>

¹⁶⁵ Computer Security Resource Centre 2023, *FIPS 186-5 Digital Signature Standard (DSS)*, National Institute of Standards and Technology, <https://csrc.nist.gov/pubs/fips/186-5/final>

¹⁶⁶ Rinaldi, S, Peerenboom, J & Kelly, T 2001, *Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies*, IEEE Control Systems 21, <https://doi.org/10.1109/37.969131>

¹⁶⁷ Branagan, M 2012, 'A Risk Simulation Framework for Information Infrastructure Protection' PhD thesis, Queensland University of Technology, https://eprints.qut.edu.au/51006/1/Mark_Branagan_Thesis.pdf

¹⁶⁸ Ibid.

Key Term	Definition
Prepare	The ability of the Australian telecommunications sector to anticipate, plan, problem-solve, and integrate proactive strategies and/or measures for vulnerability mitigation. This ensures that when disruptive events occur, the system efficiently mobilises and deploys the required resources, capabilities, and services, while also incorporating procedures and processes designed to protect the sector from disruption. ¹⁶⁹
Recover	The ability of the Australian telecommunications sector to implement short and medium-term strategies and/or measures to restore or improve the viability of the assets and services for the overall purpose of the sector. ¹⁷⁰
Sector Resilience	<p>Resilience in the Australian telecommunications sector is the ability to sustain performance in the face of unspecific and possibly unforeseen disruptive events, and to continue the provision of a critical services to a variety of end-users across the nation.¹⁷¹</p> <p>Resilience is enabled by the capacity to manage the phases of disruption: to prepare, absorb, adapt, respond, recover, learn and transform from disruptions in a timely and efficient manner.¹⁷²</p>
Respond	The ability of the Australian telecommunications sector to take actions in anticipation of, during, or immediately after a disruptive event to ensure that its consequences are mitigated and that affected stakeholders are supported as quickly as possible. ¹⁷³
Risk	Risk in the Australian telecommunications sector is: The likelihood of a disruptive event causing consequences that impact the viability of the assets and services in the telecommunications sector. Assessments of likelihood and consequence are impacted by degrees of uncertainty.
Stakeholder	An individual or organisation that has a right, share, claim, or interest in the Australian telecommunications sector. This includes but is not limited to: end users, end user organisations, supporters, developers, customers, producers, trainers, maintainers, disposers, acquirers, suppliers, regulatory bodies, and people influenced positively or negatively by a system. ¹⁷⁴
System	Combination of interacting entities organised to achieve one or more stated purposes.

169 Department of the Prime Minister and Cabinet 2022, *Australian Government Crisis Management Framework*,

<https://www.pmc.gov.au/sites/default/files/resource/download/australian-government-crisis-management-framework.pdf>

McEntire, D & Myers, A 2004, 'Preparing Communities for Disasters: Issues and Processes for Government Readiness', *Disaster Prevention and Management*, vol. 13, <https://doi.org/10.1108/09653560410534289>

170 Grigson, P & Klemm, D 2018, *Australian Disaster Preparedness Framework*, Department of Home Affairs, <https://www.homeaffairs.gov.au/emergency/files/australian-disaster-preparedness-framework.pdf>

171 Risk and Resilience Expert Panellist, 2024.

172 Organisation for Economic Development n.d., *Guidelines for Resilience Systems Analysis: How to Analyse Risk and Build a Roadmap to Resilience*, OECD iLibrary, https://www.oecd-ilibrary.org/development/guidelines-for-resilience-systems-analysis-how-to-analyse-risk-and-build-a-roadmap-to-resilience_3b1d3efe-en

173 Grigson, P & Klemm, D 2018, *Australian Disaster Preparedness Framework*, Department of Home Affairs, <https://www.homeaffairs.gov.au/emergency/files/australian-disaster-preparedness-framework.pdf>

174 International Organization for Standardization 2015, *ISO/IEC/IEEE International Standard - Systems and software engineering-- System life cycle processes*, <https://ieeexplore.ieee.org/document/10123367>

Key Term	Definition
Systemic Resilience	Systemic resilience is a property that arises dynamically when critical national infrastructure can provide agreed critical services despite internal or external disruption. The goal of systemic resilience should reflect the nation's ambitions for uninterrupted critical services (i.e. a shared vision)
The telecommunications sector	<p>The Australian telecommunications sector is a complex socio-technical system of entities, stakeholders and assets with the purpose of enabling communication to the intended recipient through the transmission, reception and/or delivery of information or data (the Purpose).</p> <p>The assets that serve this purpose are tangible (e.g. a physical item, such as hardware, computing platform, network device, or other technology component) and intangible (e.g. human effort, data, information, software, capabilities, functions, services, intellectual property (trademarks, copyright patents), images, or reputation) (Assets).</p> <p>These assets enable the delivery of communications (as data or voice signals) via services (carriage services, including cloud services) over networks, including physical or fixed networks, mobile or wireless networks (Services).</p> <p>Entities are the individuals (persons), organisations, devices or processes that underpin assets and the delivery of services (Entities).¹⁷⁵</p> <p>The sector is made up of stakeholders that provide these Services and/or Assets for the Purpose, their supply chains, as well as consumers and regulators (e.g. end-users, end-user organisations, supporters, developers, acquirers, suppliers, regulatory bodies, and people influenced positively or negatively by it) (Stakeholders).¹⁷⁶</p> <p>How well the system fulfills its purpose depends on sustaining a number of objectives (e.g. interconnectivity, continuity, availability, productivity, quality (speed, latency, priority) related to performance (Performance).</p> <p>The value of the sector is determined by stakeholders in consideration of loss of performance across the entire system life cycle or over a particular time period. These value considerations have technical, organisational, social, economic, and national security dimensions (Value).¹⁷⁷</p>
Threshold	Values are used to establish concrete decision points and operational control limits to trigger management action and response escalation. ¹⁷⁸
Transform	The ability of the Australian telecommunications sector to fundamentally change, culminating in a new system state. This may include aligning with the principles of sustainable development and 'build back better'. ¹⁷⁹

175 Computer Security Resource Centre 2023, *FIPS 186-5 Digital Signature Standard (DSS)*, National Institute of Standards and Technology, <https://csrc.nist.gov/pubs/fips/186-5/final>

176 International Organization for Standardization 2015, *ISO/IEC/IEEE International Standard - Systems and software engineering-- System life cycle processes*, <https://ieeexplore.ieee.org/document/10123367>

177 Ross, R, Pillitteri, V, Graubart, R, Bodeau, B & McQuaid, R 2021, *Developing Cyber-Resilient Systems: A Systems Engineering Approach*, National Institute of Standards and Technology, <https://doi.org/10.6028/nist.sp.800-160v2r1>

178 NIST Computer Security Resource Center 2017, *NIST IR 8183 Cybersecurity Framework Manufacturing Profile*, <https://csrc.nist.gov/pubs/ir/8183/upd1/final>

179 Department of the Prime Minister and Cabinet 2022, *Australian Government Crisis Management Framework*, <https://www.pmc.gov.au/sites/default/files/resource/download/australian-government-crisis-management-framework.pdf>
 Organisation for Economic Development n.d., *Guidelines for Resilience Systems Analysis: How to Analyse Risk and Build a Roadmap to Resilience*, OECD iLibrary, https://www.oecd-ilibrary.org/development/guidelines-for-resilience-systems-analysis-how-to-analyse-risk-and-build-a-roadmap-to-resilience_3b1d3efe-en

Appendix B. Methodologies

Method overview

This Profile is the product of four interlinked methodological steps that established the means and collected the evidence required to profile resilience in the telecommunications sector. Prior to step 1, we defined what resilience covers when referring to the telecommunications sector (see Part 1 above).

- **Step 1:** Defining the sector as a complex socio-technical system.
- **Step 2:** Before disruption: risk management and situational awareness of the risk horizon (threats, threat sources, and vulnerabilities).
- **Step 3:** During and after disruption: building consequence management capabilities.
- **Step 4:** Transforming across the phases of disruption management: lessons management and maturing sector resilience capacities.

Throughout the project, an independent 26-member Expert Panel were consulted and provided guidance and feedback.¹⁸⁰

Development of the methodology involved a literature review,¹⁸¹ a stakeholder questionnaire, a two-day Risk and Resilience Symposium, and consultations with 202 individuals across all levels of Australian government, industry and dependent and interdependent sectors. All activities were held under the Chatham House Rule, where neither the identity nor affiliation of the speaker is identified.

Each methodological step is summarised briefly below and outlined in detail in Appendix B, alongside assumptions and limitations in Appendix C.

1. Defining the sector as a complex socio-technical system

Process: Developed working definitions of the sector and key concepts by identifying relevant literature on the factors of risk (threats, threat sources, and vulnerabilities),¹⁸² and OECD Systems Analysis Guidance.¹⁸³

- an initial literature review
- a questionnaire with 107 responses
- conducting 29 semi-structured interviews with leading experts across the sector.

Output: PESTLE and Gap Analysis Report,¹⁸⁴ and *Part 2 – Evidence in Support of the Assessment* below.

2. Before disruption: risk management and situational awareness of the risk horizon (threats, threat sources, and vulnerabilities)

Process: Developed further definitions and analytical categories by:

- drawing extensively on the work of Branagan, Barnes, OECD Systems Analysis Guidelines¹⁸⁵
- mapping relevant threat and vulnerability taxonomies
- consulting with 102 individuals representing 57 organisations, using semi-structured interviews to gather evidence.

Output: The **TPDC Threat Taxonomy, Threat Source Categories**, and **TPDC Vulnerability Categories** to categorise the evidence collected, as presented in *Part 3 – Evidence in Support of the Assessment, Step 2: Prepare and Absorb* below.

¹⁸⁰ See Appendix E for full list of Risk and Resilience Experts.

¹⁸¹ See Appendix D for Suggested Reading list.

¹⁸² Branagan, M 2012, 'A Risk Simulation Framework for Information Infrastructure Protection' PhD thesis, Queensland University of Technology, https://eprints.qut.edu.au/51006/1/Mark_Branagan_Thesis.pdf

¹⁸³ Organisation for Economic Development n.d., *Guidelines for Resilience Systems Analysis: How to Analyse Risk and Build a Roadmap to Resilience*, OECD iLibrary, https://www.oecd-ilibrary.org/development/guidelines-for-resilience-systems-analysis-how-to-analyse-risk-and-build-a-roadmap-to-resilience_3b1d3efe-en

¹⁸⁴ Curtis, H & Harpley, C 2023, *Telecommunications Sector Risk and Resilience Profile: PESTLE and Gap Analysis*, ANU Tech Policy Design Centre, https://techpolicydesign.au/wp-content/uploads/2023/08/230815_TPDC_Stage-1_Teleco-Risk-Resilience_Spread.pdf

¹⁸⁵ Branagan, M 2012, 'A Risk Simulation Framework for Information Infrastructure Protection', Queensland University of Technology, https://eprints.qut.edu.au/51006/1/Mark_Branagan_Thesis.pdf

Barnes, P 2016, *Training Material at the Australian Strategic Policy Institute*, Australian Strategic Policy Institute, Canberra.

Organisation for Economic Development n.d., *Guidelines for Resilience Systems Analysis: How to Analyse Risk and Build a Roadmap to Resilience*, OECD iLibrary, https://www.oecd-ilibrary.org/development/guidelines-for-resilience-systems-analysis-how-to-analyse-risk-and-build-a-roadmap-to-resilience_3b1d3efe-en

3. During and post-disruption: building consequence management capabilities

Process: Guidance from the Expert Panel suggested focusing on consequence management by:

- reviewing literature on global good practices
- conducting a two-day Symposium with 56 participants from 38 organisations, which utilised the Delfi method¹⁸⁶ and the Pandora Forward Looking Cell method¹⁸⁷ to conduct a four-stage scenario exercise.

Output: a capture of evidence on the current state of consequence management in the sector as presented in Part 2 – Evidence in Support of the Assessment, Step 3: Adapt, Respond, Recover below.

4. Transforming from disruption: Lessons management integrates lessons across the phases of disruption management and works to mature sector resilience capabilities

Process: The project team filled gaps in the evidence base and explored how resilience can be operationalised by:

- holding three Focus Groups with 42 participants representing 27 organisations to gather evidence on
 - policy options for building resilience capacities
 - coordination, data capability, and information sharing
 - consequence management capabilities
- reviewing literature on global good practices.

Output: The **Sector Resilience Maturity Model** to synthesise evidence of the principles, capabilities and resourcing identified by stakeholders that are needed to mature capacity across all phases of disruption management (preparedness, absorption, adaptation, response, recovery, learning, and transformation) and an Assessment of the Telecommunications sector against the model.¹⁸⁸

The below sections detail the methodological approach to developing analytical categories outlined in this Profile.

Step 1. The threat taxonomy

The TPDC Telecommunications Sector Threat Taxonomy identifies six threat categories at the sector-level: Physical, Supply Chain, Cyber & Technology, Climate & Environment, Economic, and Regulatory (see Table 25 below).

As outlined in the methodology below, the TPDC Threat Taxonomy was developed by mapping the approaches of three leading international organisations alongside information gathered through Australian industry, government, and academic stakeholders on their respective categorisation methodologies.

The objective of the TPDC Telecommunications Threat Taxonomy is to develop a common, sector-wide lexicon and underscore the importance of understanding well-established threats as well as those which, at present, receive insufficient attention.

The Taxonomy assists in identifying and categorising known, emerging and potential threats, which, in turn, aids in identifying the areas and nature of impact on critical assets and systems (i.e. vulnerabilities in critical systems).

Identification and classification of threats, alongside identification of vulnerabilities, is the backbone of almost all risk assessment methodologies.¹⁸⁹ The TPDC Threat Taxonomy helps to standardise analysis.

¹⁸⁶ International Organization for Standardization 2018, *Risk Management Guidelines*, International Organization for Standardization, Geneva.

¹⁸⁷ Danish Emergency Management Agency 2016, *Pandora Forward Looking Cell*, <https://www.brs.dk/globalassets/brs--beredskabsstyrelsen/dokumenter/krisestyring-og-beredskabsplanlagning/2020/-pandorauk-.pdf>

¹⁸⁸ See section “What is Sector Resilience?” on page 26.

¹⁸⁹ Georgios, G, Roberto, F & Muriel, S 2012, *Risk Assessment Methodologies for Critical Infrastructure Protection. Part I: A State of the Art*, JRC Technical Notes, <https://doi.org/10.2788/22260>

Launius, S 2021, *Evaluation of Comprehensive Taxonomies for Information Technology Threats*, SANS Institute, <https://www.sans.org/white-papers/38360/>

Coburn, A, Bowman, G, Ruffle, S, Foulser-Piggott, R, Ralph, D & Tuveson 2014, *A Taxonomy of Threats for Complex Risk Management*, University of Cambridge, <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-cambridge-taxonomy-threats-complex-risk-management.pdf>

Table 25. Tech Policy Design Centre telecommunications threat taxonomy

Physical	Supply Chain	Cyber & Technology
<p>Threats in this category may be related to property, including: loss or theft, outages, destruction, sabotage, or vandalism.</p> <p>They may also be related to physical systems including electrical, structural facilities, water distribution, sanitation, natural gas or electronic media.</p>	<p>Threats in this category may be related to dependencies, including: supplier viability, logistics provision, including over-reliance, route disruption, provider failure, technology services.</p>	<p>Threats in this category may be related to hardware, software and systems, including: hardware capacity, performance, maintenance and obsolescence; software compatibility, configuration management, change control, cyber security, development, and coding practices and testing.</p>
Climate & Environment	Economic	Regulatory
<p>Threats in this category may be related to environmental or climatic conditions, including: fire, flood, cyclone, storm, hurricane, heat, snow, earthquake, pollution, dust, radiation, space weather, wildlife, pandemic.</p>	<p>Threats in this category may be related to economic and market conditions, including: inflation and deflation, market access, labour supply and skills availability, market structure, ownership and control, trade orientation, technological level.</p>	<p>Threats in this category may be related to legal and regulatory conditions, including: regulatory compliance, legislation, litigation, intellectual property, consumer protection, health and safety, taxation, privacy, data security.</p>

Why existing approaches are not fit-for-purpose

This project defines the telecommunications sector broadly. It includes large, medium, and small entities, and some non-traditional entities in that they do not currently fall under the remit of telecommunications legislation.

Within the Australian telecommunications sector, different entities have distinct terminology for describing strategic concerns (variously and contradictorily described as risk, threats and hazards). Descriptors are often distinct to market size, industry vertical, technology type, and jurisdiction.

There is no single authoritative threat taxonomy for the telecommunications sector, but there are several glossaries or lexicons of security terms published by a variety of governing bodies and standards organisations.¹⁹⁰

At the regulatory level, the Australian Security of Critical Infrastructure Rules 2023 identifies several relevant frameworks and obligations for critical infrastructure assets in eleven classes.¹⁹¹ These frameworks are predominately security-related and, until November 2023, did not apply to the telecommunications sector.

All frameworks and their relevant methodologies differ, based on the audience to which they are addressed (policymakers, industry decision-makers, research institutes) and their domain of applicability (asset-level, infrastructure/system level, system of systems level).¹⁹² These attributes are not necessarily mutually exclusive but can mean unavoidable generality, especially when causality is difficult to ascertain and when a single threat may cause multiple consequences due to multiple vulnerabilities.

Existing critical infrastructure risk assessment methodologies can be divided into two major categories: sectoral methodologies and systems approaches.¹⁹³

190 Launius, S 2021, *Evaluation of Comprehensive Taxonomies for Information Technology Threats*, SANS Institute, <https://www.sans.org/white-papers/38360/>

191 Department of Home Affairs 2023, *Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Rules (LIN 23/006)*.

192 Georgios, G, Roberto, F & Muriel, S 2012, *Risk Assessment Methodologies for Critical Infrastructure Protection. Part I: A State of the Art*, JRC Technical Notes, <https://doi.org/10.2788/22260>

193 Ibid.

The TPDC Telecommunications Threat Taxonomy creates a common lexicon encompassing the breadth of threats that may impact the sector, and the cross-sectoral challenges in interdependent systems.

Bringing together sectoral methodologies and systems approaches in the TPDC Telecommunications Threat Taxonomy ensures that the final profile will consider risk and resilience of the telecommunications sector in context.

Methodology: Mapping against existing model categories

To develop the TPDC Telecommunications Threat Taxonomy, the project team:

- selected three prominent international and one national model as reference taxonomies
- assessed alignment of the threat categories in the reference taxonomies with the threat definition and risk horizon model outlined in Stage One
- selected categories that aligned with the Factors in Risk model as a threat (and not as a threat source, event, vulnerability or consequence)
- included categories relevant to the telecommunications sector.

The three leading international models reviewed were from: National Institute of Standards and Technology (NIST), the European Union Agency for Cybersecurity (ENISA) and the Open Threat Typology (OTT).¹⁹⁴ These models provide standardised guidelines to help governments, industries, and organisations worldwide identify, mitigate, and manage threats.

The project team also considered existing Australian frameworks: the *Security of Critical Infrastructure Act 2018* (Cth) and the Australian Department of Home Affairs Critical Infrastructure Resilience Strategy.¹⁹⁵

The subject categories from these existing models were mapped to form the basis of the TPDC Threat Taxonomy Categories.

Table 26 maps the subject categories from these existing taxonomies alongside the categories in the TPDC Telecommunications Threat Taxonomy.

Table 27 provides a high-level overview of the differences between the TPDC taxonomy and existing approaches.

194 Ross, R, Pillitteri, V, Graubart, R, Bodeau, B & McQuaid, R 2021, *Developing Cyber-Resilient Systems: A Systems Engineering Approach*, National Institute of Standards and Technology, <https://doi.org/10.6028/nist.sp.800-160v2r1>
European Union Agency for Cybersecurity 2022, *Annual report telecom security incidents 2021*, Publications Office of the European Union, <https://op.europa.eu/en/publication-detail/-/publication/d173c7f1-0eec-11ed-8fa0-01aa75ed71a1/language-en/format-pdf#>

195 Department of Home Affairs 2023, *Critical Infrastructure Resilience Strategy*, <https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-resilience-strategy-2023.pdf>

Table 26. Mapping threat taxonomies: TPDC, NIST, Home Affairs, OTT, ENISA

TPDC Threat Taxonomy	National Institute of Standards and Technology (NIST)	European Union Agency for Cybersecurity (ENISA)	Open Threat Typology (OTT)	Critical Infrastructure Risk Management Program (Home Affairs)
Physical	<ul style="list-style-type: none"> • Actions of people 	<ul style="list-style-type: none"> • Outages • Physical attack (deliberate/intentional) 	<ul style="list-style-type: none"> • Physical threats 	<ul style="list-style-type: none"> • Physical security and natural
Supply Chain	<ul style="list-style-type: none"> • External Events 		<ul style="list-style-type: none"> • Resource threats 	<ul style="list-style-type: none"> • Supply chain
Cyber and Technology	<ul style="list-style-type: none"> • Systems and Technology Failures 	<ul style="list-style-type: none"> • Failures and Malfunction • Eavesdropping, Interception and Hijacking • Unintentional damage/loss of information or IT assets • Nefarious activity/abuse 	<ul style="list-style-type: none"> • Technical threats 	<ul style="list-style-type: none"> • Cyber and information security
Climate and Environment	<ul style="list-style-type: none"> • External Events 	<ul style="list-style-type: none"> • Disaster (natural, environmental) 		<ul style="list-style-type: none"> • Physical security and natural
Regulatory	<ul style="list-style-type: none"> • External Events 	<ul style="list-style-type: none"> • Legal 		
Economic	<ul style="list-style-type: none"> • External Events 			
Outliers	<ul style="list-style-type: none"> • Adversarial • Actions of People • Non-Adversarial • Failed Internal Processes • Service dependencies 		<ul style="list-style-type: none"> • Personnel threats 	<ul style="list-style-type: none"> • Personnel

Table 27. TPDC threat taxonomy and description

TPDC Threat Taxonomy	Description
Physical	The TPDC Physical category adopts aspects from all taxonomies. Home Affairs categorises physical security alongside natural hazard vectors. Other international taxonomies identify Physical and Natural as separate categories.
Supply Chain	The TPDC Supply Chain category has been influenced primarily by the OTT model. The OTT classifies supply chain issues as resource threats and draws attention to dependencies and disruptions. Supply chain issues are also reflected in the Home Affairs model and in their activities and reflects Australia's current strong dependence on international suppliers.
Cyber and Technology	The TPDC Cyber and Technology category adopts aspects of the NIST model, which makes a distinction between hardware, software, and systems.
Climate and Environment	The TPDC Climate and Environment category adapts to the neglect of environmental threats in all of the chosen reference models. The choice of terminology reflects this statement from the Royal Commission into National Natural Disaster Arrangements: "The expression 'natural disaster' is something of a misnomer, in part because some naturally occurring hazards (such as fires and earthquakes) may only turn into a disaster because of what humans do and fail to do."
Regulatory	The TPDC Regulatory category uses aspects of NIST, which identifies regulatory compliance as a threat. Consultation with stakeholders lead TPDC to conclude that the role of Australian government in setting regulatory frameworks required a separate category.
Economic	The TPDC category uses aspects of the NIST models, which identify market and economic and supplier failure as threats. Other reference models do not reflect this.

Step 2. The vulnerability categories

Vulnerabilities are generally classified according to the asset class to which they relate: hardware, software, network, personnel, physical, and organisational factors.¹⁹⁶

For critical assets, services and systems, Barnes posits that the elements that create vulnerabilities can be simplified into three vulnerability-creating elements: human, virtual, or physical (see Table 28).¹⁹⁷

For the purposes of this project, TPDC has adopted the simplified vulnerability-creating categories, which complement the threat categories developed in the TPDC Telecommunications Sector Threat Taxonomy (discussed above).

Why existing approaches are not fit-for-purpose

- **Traditional classification:** Existing approaches classify vulnerabilities according to detailed asset classes such as hardware, software, network, personnel, physical, and organisational factors. This detailed classification can be overly complex.
- **Lack of focus on what creates vulnerabilities:** The traditional classification methods do not focus on vulnerability-creating elements.
- **Fragmented understanding:** Current regulations and classification systems result in fragmented understandings of vulnerabilities across the sector.

This simplification facilitates a more straightforward understanding and management of vulnerabilities. By creating a common language for the sector and emphasising the sources of vulnerability, this approach can allow for more targeted and effective mitigation strategies.

Methodology: Developing the categories

- **Review of existing classifications:** The process began with a review of existing vulnerability classifications according to *ISO/IEC 27005:2018*, identifying asset classes such as hardware, software, network, personnel, physical, and organisational factors.
- **Simplification by Barnes:** Based on Barnes's framework, vulnerabilities were re-categorised into three simplified elements: human, virtual, and physical. This approach reduces complexity and aligns with the sector's needs.

Table 28. Mapping vulnerability categories

Vulnerability creating categories	Asset class (ISO/IEC 27005:2018)
Human	Personnel, organisational
Virtual	Software, network
Physical	Hardware, physical

¹⁹⁶ International Organization for Standardization and International Electrotechnical Commission 2021, *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks*, <https://www.iso.org/standard/80585.html>

¹⁹⁷ Barnes, P 2016, *Training Material at the Australian Strategic Policy Institute*, Australian Strategic Policy Institute, Canberra.

Step 3. The consequence management analysis

Development of the consequence management analysis for the telecommunications sector is rooted in the guidance provided by the Expert Panel. This analysis shifts the focus from traditional risk management to consequence management. The following methodology outlines the process undertaken to conceptualise, develop, and validate the Consequence Management Analysis.

Why existing approaches are not fit-for-purpose

- **Persistent uncertainties:** Despite robust risk management practices, uncertainties and unexpected events continue to occur. Consequence management acknowledges these uncertainties and focuses on managing the myriad potential impacts of disruptions.
- **Maturity imbalance:** The telecommunications sector is more advanced in risk management than in consequence management. However, this focus has not necessarily produced sectoral resilience capacities across the phases of disruption management.
- **Threat-agnostic strategy:** By concentrating on threat-agnostic consequence management, the sector can enhance its ability to respond to disruptions swiftly and decisively, regardless of the unpredictable nature of the risk horizon.
- **Alignment with government activities:** A consequence management approach aligns with broader government activities at local, state and federal levels.
- **Fragmented capabilities:** Industry consultations revealed that current regulations lead to fragmented capabilities, impeding service continuity during disruptions. Developing sector-specific guidance for consequence management is essential for telecommunications entities.

Methodology: Developing the analysis

Literature review:

- **OECD Guidelines:** Reviewed OECD Critical Infrastructure Resilience Guidelines to identify system-level qualities that mitigate impacts, especially where service continuity responsibilities span both private and government sectors.¹⁹⁸
- **Broader literature:** Examined literature on consequence management and business continuity practices, identifying key activities such as training, exercises, coordination, learning, information management, and inter-agency collaboration.

Connecting sector and enterprise-levels:

- **Systems thinking:** Applied a systems-thinking perspective to profile the current and future states of consequence management, based on focus group evidence.
- **Organisational resilience:** Leveraged the Department of Home Affairs Cyber and Infrastructure Security Centre's Organisational Resilience Good Practice Guide, which emphasises adaptability and sustainability.¹⁹⁹

¹⁹⁸ Organisation for Economic Development n.d., *Guidelines for Resilience Systems Analysis: How to Analyse Risk and Build a Roadmap to Resilience*, OECD iLibrary, https://www.oecd-ilibrary.org/development/guidelines-for-resilience-systems-analysis-how-to-analyse-risk-and-build-a-roadmap-to-resilience_3b1d3efe-en

¹⁹⁹ Department of Home Affairs 2024, *Organisational Resilience: Good Practice Guide*, <https://www.cisc.gov.au/how-we-support-industry-subsite/Documents/org-res-good-practice-guide.pdf>

Evidence base collection:

An eight-stage process was followed to assemble the evidence base:

- **Literature review:** Conducted a comprehensive review of literature on consequence management and critical infrastructure resilience.
- **Narrative framework:** Produced a two-page narrative document for feedback from the Expert Panel.
- **Expert Panel input:** Sought input and tested ideas with the Expert Panel.
- **Symposium:** Hosted a Symposium on Risk and Resilience in the Telecommunications Sector. The Symposium brought together over 60 participants from academia, industry and government across the country to discuss the resilience of telecommunications in Australia and the consequences of disruption.
- **Hypothesis development:** Developed hypotheses on resilience policies, crisis management, and thresholds, based on panel feedback.
- **Focus group design:** Designed focus groups based on literature, hypotheses, and Expert Panel input.
- **Focus groups execution:** Held focus groups with diverse participants from across the sector, as well as dependent and interdependent sectors.
- **Thematic analysis:** Employed qualitative analysis techniques to identify key considerations informing consequence management.
- **Analysis development:** Used findings from focus groups to develop the Consequence Management Capability Analysis.

Focus group method:

Three focus groups were organised, each focusing on a critical topic identified by the Expert Panel:

- Resilience policy
- Information-sharing, data capability, and coordination
- Decision-making thresholds during disruption.

Outcome: The focus groups yielded valuable insights on resilience capabilities and consequence management practices, forming the foundation for developing the Consequence Management Capability Analysis. This provided a framework for the sector to enhance its capacity to respond to and recover from disruptions.

Step 4. The sector resilience maturity model

Why existing approaches are not fit-for-purpose

The development of the Sector Resilience Maturity Model (SRMM) for the Australian telecommunications sector was guided by the need to have: (1) a model for profiling resilience concepts, (2) provide decision-makers with a model to assess and enhance sectoral resilience.

Maturity models are valuable assessment tools that enable the enhancement of the quality of a subject of interest. Organisations can use these models to evaluate their strengths and weaknesses, such as their level of organisational resilience, and create targeted improvement roadmaps. Additionally, maturity models allow organisations to assess the effectiveness of implemented improvement measures.²⁰⁰

While resources like the Cyber Infrastructure Security Centre's Organisational Resilience Good Practice Guide²⁰¹ and the United Nations' Organisational Resilience Maturity Model²⁰² support resilience at the organisational level, there is a critical gap in applying these lessons, operationalising resilience, and driving transformation at the sector-level.

Moreover, despite widespread discussions on bolstering sectoral resilience through capacity building, capability enhancement, and resource allocation, there is an absence of national strategies to realise these objectives.

The SRMM bridges the gap between conceptual aspirations and actionable strategies by integrating the notions of enhancing resilience capacities with the fundamental principles, capabilities, and resources necessary to facilitate the embedding of lessons learned, and foster transformative change within the sector.

Structured around three key components: resilience principles, resilience capabilities, and resilience resources—the sRMM facilitates evaluation across five maturity levels, from initial to optimised.

Methodology

To develop the sRMM, the following steps were undertaken:

1. **Conceptualisation:** feedback from the project's Expert Panel (RREP) identified the gaps outlined above. From there, the project team identified the key dimensions of resilience capacities, including principles, capabilities and resources, adapting and building upon the United Nations Office for Disaster Risk Reduction's *Principles for resilient infrastructure*²⁰³ body of work.
2. **Review of existing models:** A review of existing resilience maturity models published within the past five years was conducted to identify relevant frameworks and best practices (see Table 29 on next).
3. **Alignment assessment:** The identified models were assessed for their alignment with the specific context and needs of the Australian telecommunications sector. This assessment focused on identifying elements that directly addressed the sector's risk and resilience challenges and could be incorporated into the RMM.
4. **Evidence analysis:** Primary evidence collected through stakeholder consultation, especially in the Stage 4 Focus Groups and Stage 4 RREP meeting, was analysed and informed the development of the model.
5. **Integration of relevant elements:** Elements from the reviewed models that were directly relevant to the resilience of the Australian telecommunications sector were integrated into the RMM. These elements informed the definition of key principles, capabilities, and resources within the model, ensuring its practical applicability to the sector.

200 Durst, S, Henschel, T 2024, *Small and Medium-Sized Enterprise (SME) Resilience: Strategies for Risk and Crisis Management*, Google Books, https://books.google.com.au/books?hl=en&lr=&id=1F38EAAQBAJ&oi=fnd&pg=PR8&ots=0EFRkKgiCF&sig=Okzfp3fC_UiVaOqF8FZmZtPYICA&redir_esc=y#v=onepage&q&f=false

201 Department of Home Affairs 2024, *Organisational Resilience: Good Practice Guide*, <https://www.cisc.gov.au/how-we-support-industry-subsite/Documents/org-res-good-practice-guide.pdf>

202 United Nations System Chief Executives Board for Coordination n.d., *UN Organizational Resilience Maturity Model*, Addison-Wesley Professional, <https://unsceb.org/sites/default/files/2021-12/Approved%20Organizational%20Resilience%20Maturity%20Model.pdf>

203 United Nations Office for Disaster Risk Reduction 2021, *Principles for Resilient Infrastructure*, <https://www.undrr.org/publication/principles-resilient-infrastructure>

Table 29. Existing resilience maturity models

Year	Author	Title of Model
2024	Department of Home Affairs' Cyber and Infrastructure Security Centre	Organisational Resilience: Good Practice Guide ²⁰⁴
NA	The United Nations System Chief Executives Board for Coordination	UN Organizational Resilience Maturity Model ²⁰⁵
2024	Nadine Otter and Mark Uschkurat	Conceptual Development of a Resilience Maturity Model for SMEs ²⁰⁶
2021	Shaked et al	Incorporating systems thinking into a cyber resilience model ²⁰⁷
2019	Hernantes J et al.	Towards resilient cities: A maturity model for operationalizing resilience ²⁰⁸

By following this methodology, the SRMM was systematically developed to provide the project team with a useful profiling model, and decision-makers and policymakers with a robust framework for assessing and enhancing the resilience of the Australian telecommunications sector. The model's comprehensive design enables stakeholders to evaluate resilience across its various components and maturity levels, ultimately supporting the sector's ability to manage disruptions and thrive in an ever-changing environment.

204 Department of Home Affairs 2024, *Organisational Resilience: Good Practice Guide*, <https://www.cisc.gov.au/how-we-support-industry-subsite/Documents/org-res-good-practice-guide.pdf>

205 United Nations System Chief Executives Board for Coordination n.d., *UN Organizational Resilience Maturity Model*, Addison-Wesley Professional, <https://unsceb.org/sites/default/files/2021-12/Approved%20Organizational%20Resilience%20Maturity%20Model.pdf>

206 Otter, N & Uschkurat, M 2024, *Conceptual Development of a Resilience Maturity Model for SMEs*, Springer, https://books.google.com.au/books?hl=en&lr=&id=1F38EAAQBAJ&oi=fnd&pg=PR8&ots=0EFRkKgiCF&sig=Okzfp3fC_UIVaOqF8FZmZtPYICA&redir_esc=y#v=onepage&q&f=false

207 Shaked, A, Tabansky, L & Reich Y 2020, 'Incorporating Systems Thinking Into a Cyber Resilience Maturity Model', IEEE Journals & Magazine vol. 1, <https://ieeexplore.ieee.org/document/9302574>

208 Hernantes, J, Marañá, P, Gimenez, R, Sarriegi, J & Labaka, L 2019, 'Towards Resilient Cities: A Maturity Model for Operationalizing Resilience', Cities, vol. 84, <https://doi.org/10.1016/j.cities.2018.07.010>

Appendix C. Assumptions and limitations

The Profile of evidence is presented with the following assumptions and limitations:

Table 30. Assumptions and limitations

	Assumptions	Limitations
Uncertainty and ambiguity	The inherent complexity of the telecommunications sector is assumed. The dynamic nature of its risk horizon is assumed to introduce significant uncertainty and ambiguity.	<p>The ever-evolving nature of the telecommunications sector and its environment means that new threats, threat sources, and vulnerabilities can emerge, and existing threats and vulnerabilities can change in character or significance.</p> <p>While the models and analysis developed provide valuable insights, they cannot eliminate these uncertainties.</p>
Comprehensiveness of evidence and temporal factor	The threats, threat sources, vulnerabilities, and disruptions identified through the literature review, consultations, and interviews represent a comprehensive snapshot of the current risk horizon within the telecommunications sector.	Despite extensive efforts to capture the full scope of factors of risk, there are inevitably unknown threats, threat sources, vulnerabilities, and potential disruptions that were not identified during the course of this project. The evidence may not reflect future developments or emerging threats.
Sector definition	The telecommunications sector can be accurately defined and analysed as a complex socio-technical system. This assumption underpins the development of the working definitions and analytical frameworks used throughout the project.	Although extensive, the consultations and interviews may not cover all possible perspectives within the sector, particularly those from smaller or less-represented organisations.

	Assumptions	Limitations
Consultative method	<p>The Expert Panel's insights and feedback and the extensive sector consultations provide a thorough and representative understanding of the telecommunications sector's resilience capabilities and needs.</p> <p>The consultations, focus groups, and symposium conducted under the Chatham House Rule are assumed to have encouraged candid and honest contributions from participants, which are critical for the accuracy and depth of the findings.</p>	<p>While invaluable, the guidance and feedback from the 26-member Expert Panel may introduce biases based on the panel's composition and viewpoints.</p> <p>The reliance on semi-structured interviews, focus groups, and literature reviews means that the findings are subject to the limitations inherent in qualitative research, such as potential biases in participant responses and interpretation of data.</p> <p>While the Chatham House Rule likely encouraged openness, it also means that specific contributions cannot be attributed, potentially limiting the ability to follow up on or validate particular insights or claims.</p>
Generalisability	<p>The methods and categories such as the TPDC Threat Taxonomy, TPDC Threat Source Categories, and TPDC Vulnerability Categories are assumed to be consistently applicable and reliable across different segments of the telecommunications sector.</p>	<p>The categories and frameworks developed, while robust, may not be universally applicable across all regions or contexts beyond the scope of the Australian telecommunications sector. Differences in regulatory environments, market conditions, and technological infrastructure may limit their broader applicability.</p>

Appendix D. Suggested reading

Recommended reading on risk and resilience

- Branagan, M 2012, 'A Risk Simulation Framework for Information Infrastructure Protection' PhD thesis, Queensland University of Technology, https://eprints.qut.edu.au/51006/1/Mark_Branagan_Thesis.pdf
- Organisation for Economic Development n.d., *Guidelines for Resilience Systems Analysis: How to Analyse Risk and Build a Roadmap to Resilience*, OECD iLibrary, https://www.oecd-ilibrary.org/development/guidelines-for-resilience-systems-analysis-how-to-analyse-risk-and-build-a-roadmap-to-resilience_3b1d3efe-en
- Organisation for Economic Development 2019, *OECD Reviews of Risk Management Policies: Good Governance for Critical Infrastructure Resilience*, OECD iLibrary, <https://www.oecd-ilibrary.org/sites/02f0e5a0-en/index.html?itemId=/content/publication/02f0e5a0-en>
- United Nations Office for Disaster Risk Reduction 2021, *Principles for Resilient Infrastructure*, <https://www.undrr.org/publication/principles-resilient-infrastructure>
- Pursiainen, C & Kytömaa, E 2022, 'From European Critical Infrastructure Protection to the Resilience of European Critical Entities: What Does It Mean', *Sustainable and Resilient Infrastructure*, vol. 8, <https://doi.org/10.1080/23789689.2022.2128562>
- Osei-Kyei, R, Almeida, L, Ampratwum, G & Tam, V 2022, 'Systematic Review of Critical Infrastructure Resilience Indicators', *Construction Innovation*, vol. 23 no. 5, <https://doi.org/10.1108/ci-03-2021-0047>
- *Recommended reading on consequence and consequence management*
- Pescaroli, G & Alexander, D 2018, 'Understanding Compound, Interconnected, Interacting, and Cascading Risks: A Holistic Framework', *Risk Analysis* vol. 38, <https://doi.org/10.1111/risa.13128>
- Danish Emergency Management Agency 2016, *Pandora Forward Looking Cell*, <https://www.brs.dk/globalassets/brs---beredskabsstyrelsen/dokumenter/krisestyring-og-beredskabsplanlagning/2020/-pandorauk-.pdf>
- Crosweiler, M n.d., *Improving Our Capability to Better Plan for, Respond to, and Recover From Severe-to-catastrophic Level Disasters*, Australian Disaster Resilience Knowledge Hub, <https://knowledge.aidr.org.au/resources/ajem-oct-2015-improving-our-capability-to-better-plan-for-respond-to-and-recover-from-severe-to-catastrophic-level-disasters/>

Recommended reading on lessons management

- Crawley, H, Eburn, M, Logan, K, Beekharry, D, Strickland, R, Thomason, M & Males, J 2019, *Lessons Management Handbook*, Australian Institute for Disaster Resilience, https://www.aidr.org.au/media/1760/aidr_handbookcollection_lessonsmanagement_2019.pdf

Recommended reading on interdependencies

- Rinaldi, S, Peerenboom, J & Kelly, T 2001, 'Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies', *IEEE Control Systems*, vol. 21, <https://doi.org/10.1109/37.969131>

Appendix E. Risk and Resilience Expert Panel Members

Alexander Osborne	Fred Fernandes (Observer, Risk Advisor)	Luke Coleman
Cameron Scott	Dr Gareth Downing	Michelle Phillips
Carolyn Phiddian	Gill Savage	Min Livanidis
Chloe Harpley (Observer, Project Manager)	Dr Holly Randell-Moon	Narelle Clark
Colin Muller	Dr Huon Curtis (Observer, Lead Researcher)	Dr Paul Barnes
Craig Smith	Jamie Morse	Professor Ryan Ko
Dave O’Loan	Jason Duerden	Stephen Farrugia
Dan Weis	Jeff Whitton	Representative from the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (ex officio)
David Haigh	Professor Johanna Weaver (Chair)	
Ebony Aitken	Kirsty McKinnon	
Elise Ball	Laurence Plant	Representative from the Department of Home Affairs (ex officio)

All members served in their independent capacity as experts.

Appendix F. Stakeholders consulted

Table 31. Organisations consulted throughout the project

Organisations

AARNet	Internet Association of Australia
ABC	Macquarie Telecom
ACT Emergency Management	National Emergency Management Agency
Amazon Web Services	National Space Agency
Ambulance Service of Western Australia	NBN Co
ANU School of Cybernetics	Nexon
Aussie Broadband	Nokia
Australian Communications and Media Authority (ACMA)	Northern Territory Government
Australian Communications Consumer Action Network (ACCAN)	NSW Telco Authority
Australian Risk Policy Institute	Optus
Australian Space Agency	Pivotel
BAI Communications	Police Force
Charles Sturt University	Queensland Department of Communities, Housing and Digital Economy (CHDE)
CI-ISAC	Sabre Net
Commpete	SentinelOne
Communications Sector Group members	South Australian Dept. of Premier and Cabinet
CSIRO Data61	South Australian Dept. of Primary Industries and Regions
Department of Climate Change, Energy, the Environment and Water	Tait Communications
Dept. of Home Affairs	Tasmanian Dept. of Premier and Cabinet
Dept. of Industry, Science & Resources (Office of Supply Chain Resilience)	Telstra
Dept. of Infrastructure, Transport, Regional Development, Communications and the Arts	TPG Telecom
Dept. of the Prime Minister and Cabinet	University of Technology Sydney
Ericsson	UQ Cyber – University of Queensland
Essential Energy	Ventia
Griffith University	Victorian Department of Jobs, Precincts and Regions
IBM	Victorian Dept. of Government Service
Independent Cyber Expert	Vocus
Independent Energy Expert	WaveConn
Independent Legal Expert	Western Australia Department of Biodiversity, Conservation and Attractions
Independent Regulatory Expert	Western Australian Dept. of Health
Independent Safety Expert	Western Dept. of Fire & Emergency Services
Independent Technical Expert	Wi-Sky
	Women with Disabilities Australia

Appendix G. Index of Tables

Table 1. Understanding resilience capacities across all phases of disruption management.	15
Table 2. Assessment of Australian telecommunications sector maturity against the Resilience Principles.	26
Table 3. Assessment of Australian telecommunications sector maturity against the TPDC Resilience Capabilities	28
Table 4. Assessment of Australian telecommunications sector maturity against Resilience Resources	39
Table 5. Summary of telecommunications entities and stakeholders, functions, and examples	43
Table 6. Physical threats identified by stakeholders	55
Table 7. Gaps in physical threat evidence identified by the project team	57
Table 8. Cyber threats identified by stakeholders	58
Table 9. Technological threats identified by stakeholders	60
Table 10. Gaps in cyber and technology threats identified by the project team	62
Table 11. Climate and environment threats identified by stakeholders	63
Table 12. Gaps in climate and environment threats identified by the project team	66
Table 13. Economic threats identified by stakeholders	67
Table 14. Gaps in economic threats identified by the project team	69
Table 15. Regulatory threats identified by stakeholders	70
Table 16. Supply chain threats identified by stakeholders	73
Table 17. Gaps in supply chain threats identified by the project team	75
Table 19. Non-malicious threat sources identified by stakeholders.	76
Table 20. Mapping vulnerability categories.	77
Table 21. Human-created vulnerabilities identified by stakeholders.	79
Table 22. Virtually created vulnerabilities identified by stakeholders.	81
Table 23. Physically-created vulnerabilities identified by stakeholders	83
Table 24. Capture of evidence relevant to current weaknesses in consequence management.	87
Table 25. Tech Policy Design Centre telecommunications threat taxonomy.	99
Table 26. Mapping threat taxonomies: TPDC, NIST, Home Affairs, OTT, ENISA	101
Table 27. TPDC threat taxonomy and description	102
Table 28. Mapping vulnerability categories.	103
Table 30. Assumptions and limitations.	108
Table 31. Organisations consulted.	112

Appendix H. Index of figures

Figure 1. Profiling resilience in the Australian telecommunications sector.	10
Figure 2. Resilience capacities can be built over all phases of the disruption management process for continuous learning and improvement.	16
Figure 3. Overview of the Sector Resilience Maturity Model	22
Figure 4. Schematic of the Australian telecommunications sector	48
Figure 5. Project evidence mapped against TPDC Threat Taxonomy categories	54

Appendix I. Bibliography

- Adini, B, Goldberg, A, Cohen, R, Laor, D & Bar-Dayana, Y 2012, 'Evidence-based support for the all-hazards approach to emergency preparedness', *Israel Journal of Health Policy Research*, vol. 1, no. 40, viewed 25 October 2012, <https://doi.org/10.1186/2045-4015-1-40>
- Amir, S, Salehi, N, Roci, M, Sweet, S & Rashid, A 2022, 'Towards Circular Economy: A Guiding Framework for Circular Supply Chain Implementation', *Business Strategy and the Environment*, vol. 32, no. 6, <https://doi.org/10.1002/bse.3264>
- Ampratwum, G, Osei-Kyei, R & Tam, V 2022, 'Exploring the Concept of Public-private Partnership in Building Critical Infrastructure Resilience Against Unexpected Events: A Systematic Review', *International Journal of Critical Infrastructure Protection*, vol. 39, <https://doi.org/10.1016/j.ijcip.2022.100556>
- Andrew, T.N & Petkov, D 2003, 'The Need for a Systems Thinking Approach to the Planning of Rural Telecommunications Infrastructure', *Telecommunications Policy*, vol. 27, no. 1–2, [https://doi.org/10.1016/s0308-5961\(02\)00095-2](https://doi.org/10.1016/s0308-5961(02)00095-2)
- Attaran, M 2021, *The Impact of 5G on the Evolution of Intelligent Automation and Industry Digitization*, *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 5, <https://doi.org/10.1007/s12652-020-02521-x>
- Australian Communications and Media Authority 2020, *Impacts of the 2019-20 bushfires on the telecommunications network*, <https://www.acma.gov.au/publications/2020-04/report/impacts-2019-20-bushfires-telecommunications-network>
- Australian Communications and Media Authority 2021, *Communications and media in Australia: Trends and developments in telecommunications 2022-2023*, https://www.acma.gov.au/sites/default/files/2023-12/Trends%20and%20developments%20in%20telecommunications%202022-23_0.pdf
- Australian Competition and Consumer Commission 2023, *Regional Mobile Infrastructure Inquiry*, <https://www.accc.gov.au/system/files/Regional%20Mobile%20Infrastructure%20Inquiry%20final%20report.pdf>
- Australian Journal of Emergency Management 2023, *Measuring capability maturity for severe-to-catastrophic disasters*, Australian Disaster Resilience Knowledge Hub 38, <https://knowledge.aidr.org.au/resources/ajem-january-2023-measuring-capability-maturity-for-severe-to-catastrophic-disasters/>
- Australian Resilience Centre 2021, *Transforming Systems*, <https://www.ausresilience.com.au/transforming-systems>
- Australian Signals Directorate 2023, *ASD Cyber Threat Report 2022-2023*, <https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf>
- Balmer, R, Levin, S & Schmidt, S 2020, 'Artificial Intelligence Applications in Telecommunications and Other Network Industries', *Telecommunications Policy*, vol. 44, no. 6, <https://doi.org/10.1016/j.telpol.2020.101977>
- Barnes, P 2016, *Training Material at the Australian Strategic Policy Institute*, Australian Strategic Policy Institute, Canberra.
- Barnes, P & Bergin, A 2020, *Risk, Resilience & Crisis Preparedness, After COVID 19: Australia and the World Rebuild*, Australian Strategic Policy Institute, https://www.academia.edu/43153398/Risk_Resilience_and_Crisis_Preparedness
- Baxter, G & Sommerville, I 2011, *Socio-technical Systems: From Design Methods to Systems Engineering*, Interacting With Computers, <https://doi.org/10.1016/j.intcom.2010.07.003>
- Bennett, M 2015, *Illegal Mobile Phone Signal Boosters Causing Problems for Other Network Users*, ABC News, <https://www.abc.net.au/news/2015-03-07/mobile-repeaters-disrupting-mobile-phone-signal/6287256>
- Binskin, M, Bennett, A & Macintosh A 2020, *Royal Commission into National Natural Disaster Arrangements Report*, Commonwealth of Australia, <https://www.royalcommission.gov.au/system/files/2020-12/Royal%20Commission%20into%20National%20Natural%20Disaster%20Arrangements%20-%20Report%20%20%5Baccessible%5D.pdf>
- Bradaï, A, Rehmani, M, Haque, I, Nogueira, M & Bukhari S 2020, 'Software-Defined Networking (SDN) and Network Function Virtualization (NFV) for a Hyperconnected World: Challenges, Applications, and Major Advancements', *Journal of Network and Systems Management*, vol. 28, no. 3, <https://doi.org/10.1007/s10922-020-09542-z>
- Branagan, M 2012, 'A Risk Simulation Framework for Information Infrastructure Protection' PhD thesis, Queensland University of Technology, https://eprints.qut.edu.au/51006/1/Mark_Branagan_Thesis.pdf

- Carey, E, Marley, J & Desai, H 2020, *Resilience-building in practice*, Organisation for Economic Cooperation and Development, <https://www.oecd-ilibrary.org/sites/204755cb-en/index.html?itemId=/content/component/204755cb-en>
- Cavallo, A 2013, 'Integrating disaster preparedness and resilience: a complex approach using System of Systems', *Australian Journal of Emergency Management*, vol. 29, no. 3, <https://knowledge.aidr.org.au/resources/ajem-jul-2014-integrating-disaster-preparedness-and-resilience-a-complex-approach-using-system-of-systems/>
- Chester, M, Underwood, B, Allenby, B, Garcia, M, Samaras, C, Markolf, S, Sanders, K, Preston, B & Miller, T 2021, 'Infrastructure Resilience to Navigate Increasingly Uncertain and Complex Conditions in the Anthropocene', *Npj Urban Sustainability*, vol. 1, no. 1, <https://doi.org/10.1038/s42949-021-00016-y>
- Cholda, P, Tapolcai, J, Cinkler, K, Wajda K & Jajszczyk, A 2009, 'Quality of Resilience as a Network Reliability Characterization Tool', *IEEE Network*, vol. 23, no. 2, <https://doi.org/10.1109/MNET.2009.4804331>
- Chouinard, P & Giddings, J 2023, *A Systems Approach to Critical Infrastructure Resilience*, Advanced Sciences and Technologies for Security Applications, https://doi.org/10.1007/978-3-031-21530-8_3
- Clare, M 2021, *Submarine Cable Protection and the Environment*, International Cable Protection Committee (ICPC), https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/ICPC_Public_EU_March%202021.pdf
- Coburn, A, Bowman, G, Ruffle, S, Foulser-Piggott, R, Ralph, D & Tuveson 2014, *A Taxonomy of Threats for Complex Risk Management*, University of Cambridge, <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-cambridge-taxonomy-threats-complex-risk-management.pdf>
- Coscelli, A & Thompson, G 2022, *Resilience and Competition Policy: Economics Working Paper*, Competition and Markets, GOV.UK, <https://www.gov.uk/government/publications/resilience-and-competition-policy-economics-working-paper>
- Computer Security Resource Centre 2023, *FIPS 186-5 Digital Signature Standard (DSS)*, National Institute of Standards and Technology, <https://csrc.nist.gov/pubs/fips/186-5/final>
- Conges, A, Breard, L, Patruno, W, Ouro-Sao, A, Salatge, N, Fertier, A, Lauras, M, Graham, J, Benaben, F 2023, 'Situational Awareness and Decision-making in a Crisis Situation: A Crisis Management Cell in Virtual Reality', *International Journal of Disaster Risk Reduction*, vol. 97, <https://doi.org/10.1016/j.ijdrr.2023.104002>
- Connelly, E, Allen, C, Hatfield, K, Palma-Oliveira, J, Woods, D & Linkov, I 2017, *Features of Resilience*, Environment Systems & Decisions, <https://doi.org/10.1007/s10669-017-9634-9>
- Crawley, H, Eburn, M, Logan, K, Beekhar, D, Strickland, R, Thomason, M & Males, J 2019, *Lessons Management Handbook*, Australian Institute for Disaster Resilience, https://www.aidr.org.au/media/1760/aidr_handbookcollection_lessonsmanagement_2019.pdf
- Croweller, M n.d., *Improving Our Capability to Better Plan for, Respond to, and Recover From Severe-to-catastrophic Level Disasters*, Australian Disaster Resilience Knowledge Hub, <https://knowledge.aidr.org.au/resources/ajem-oct-2015-improving-our-capability-to-better-plan-for-respond-to-and-recover-from-severe-to-catastrophic-level-disasters/>
- CSIRO 2022, *State of the Climate 2022*, CSIRO, <https://www.csiro.au/en/research/environmental-impacts/climate-change/State-of-the-Climite>
- Curtis, H & Harpley, C 2023, *Telecommunications Sector Risk and Resilience Profile: PESTLE and Gap Analysis*, ANU Tech Policy Design Centre, https://techpolicydesign.au/wp-content/uploads/2023/08/230815_TPDC_Stage-1_Teleco-Risk-Resilience_Spread.pdf
- Cyber and Infrastructure Security Centre n.d., *Legislation, regulation and compliance: Critical infrastructure security legislation*, <https://www.cisc.gov.au/legislation-regulation-and-compliance>
- Danish Emergency Management Agency 2016, *Pandora Forward Looking Cell*, <https://www.brs.dk/globalassets/brs---beredskabsstyrelsen/dokumenter/krisestyring-og-beredskabsplanlagning/2020/-pandorauk-.pdf>
- Darnhofer, I 2021, *Farming Resilience: From Maintaining States Towards Shaping Transformative Change Processes*, Department of Economics and Social Sciences Austria, <https://doi.org/10.3390/su13063387>
- Department for Digital, Culture, Media & Sport and Department for Science, Innovation & Technology 2022, *Open RAN Principles*, GOV.UK, <https://www.gov.uk/government/publications/uk-open-ran-principles/open-ran-principles>

Department of Defence 2022, *National Defence: Defence Strategic Review*, <https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review>

Department of Home Affairs 2020, *Security Legislation Amendment (Critical Infrastructure) Bill 2020*, <https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems>

Department of Home Affairs 2023, *2023–2030 Australian Cyber Security Strategy*, <https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf>

Department of Home Affairs 2023, *Critical Infrastructure Resilience Strategy*, <https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-resilience-strategy-2023.pdf>

Department of Home Affairs 2023, *Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Rules (LIN 23/006)*.

Department of Home Affairs 2024, *Guidance for the Critical Infrastructure Risk Management Program*, <https://www.cisc.gov.au/resources-subsite/Documents/guidance-for-the-critical-infrastructure-risk-management-program.pdf>

Department of Home Affairs 2024, *Organisational Resilience: Good Practice Guide*, <https://www.cisc.gov.au/how-we-support-industry-subsite/Documents/org-res-good-practice-guide.pdf>

Department of the Prime Minister and Cabinet 2022, *Australian Government Crisis Management Framework*, <https://www.pmc.gov.au/sites/default/files/resource/download/australian-government-crisis-management-framework.pdf>

Department of the Premier and Cabinet 2024, *State Emergency Management Plan*, <https://www.dpc.sa.gov.au/responsibilities/security-emergency-and-recovery-management/state-emergency-management-plan>

Department of Infrastructure, Transport, Regional Development, Communications and the Arts n.d., *NBN legislative framework*, <https://www.infrastructure.gov.au/media-technology-communications/internet/national-broadband-network/nbn-legislative-framework>

Defense Technical Information Center 2000, *DTIC ADA529128: A Common Perspective: US Joint Forces Command Joint Warfighting Center Doctrine Division's Newsletter*, Internet Archive, https://archive.org/details/DTIC_ADA529128

Duchek, S 2019, *Organizational Resilience: A Capability-based Conceptualization*, BuR – Business Research, <https://doi.org/10.1007/s40685-019-0085-7>

Durkovich, C 2020, *Protecting Critical Infrastructure*, The MIT Press eBooks, <https://doi.org/10.7551/mitpress/13831.003.0012>

Durst, S, Henschel, T 2024, *Small and Medium-Sized Enterprise (SME) Resilience: Strategies for Risk and Crisis Management*, Google Books, https://books.google.com.au/books?hl=en&lr=&id=1F38EAAAQBAJ&oi=fnd&pg=PR8&ots=0EFRkKgiCF&sig=Okzfp3fC_UIVaOqF8FZmZtPYICA&redir_esc=y#v=onepage&q&f=false

Emergency Management Victoria 2022, *Consequence Management*, <https://www.emv.vic.gov.au/responsibilities/consequence-management>

Emergency Management Victoria 2023, *Victorian Preparedness Framework*, <https://www.emv.vic.gov.au/how-we-help/emergency-management-capability-in-victoria/victorian-preparedness-framework-0>

Energy Networks Australia 2020, *Memorandum of Understanding (MoU) between Energy Networks Australia and Communications Alliance*, <https://www.energynetworks.com.au/news/ena-and-comms-alliance-mou/>

European Union Agency for Cybersecurity 2022, *Annual report telecom security incidents 2021*, Publications Office of the European Union, <https://op.europa.eu/en/publication-detail/-/publication/d173c7f1-0eec-11ed-8fa0-01aa75ed71a1/language-en/format-pdf#>

Fjäder, C 2014, 'The Nation-state, National Security and Resilience in the Age of Globalisation', *Resilience* vol. 2, <https://doi.org/10.1080/21693293.2014.914771>

Gannon, J, Tendulkar, A, Lim, C & Serentschy, G 2023, *Lessons for Canada From International Approaches to Network Resiliency and Reliability*, International Telecommunications Society (ITS), <https://www.econstor.eu/bitstream/10419/277962/1/Gannon.pdf>

- Gatti, S & Chiarella, C 2020, *The Evolution of the Telecom Infrastructure Business*, Disruption in the Infrastructure Sector: Challenges and Opportunities for Developers, Investors and Asset Managers, <https://doi.org/10.1007/978-3-030-44667-3>
- Georgios, G, Roberto, F & Muriel, S 2012, *Risk Assessment Methodologies for Critical Infrastructure Protection. Part I: A State of the Art*, JRC Technical Notes, <https://doi.org/10.2788/22260>
- Gregory, M, Scholfield, K, Ahmed, K, McLaren, D & Williams, J 2014, 'Warrnambool Exchange Fire – Resilience and Emergency Management', *Journal of Telecommunications and the Digital Economy*, vol. 2, <https://doi.org/10.7790/ajtde.v2n4.72>
- Grigson, P & Klemm, D 2018, *Australian Disaster Preparedness Framework*, Department of Home Affairs, <https://www.homeaffairs.gov.au/emergency/files/australian-disaster-preparedness-framework.pdf>
- Groenedaal, J, Helsloot, I 2020, 'Organisational Resilience: Shifting From Planning-driven Business Continuity Management to Anticipated Improvisation', *Journal of Business Continuity and Emergency Planning*, vol. 1, <https://pubmed.ncbi.nlm.nih.gov/33239142/>
- GSMA 2020, *Mobile Telecommunications Security Threat Landscape*, <https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2020/02/2020-SECURITY-THREAT-LANDSCAPE-REPORT-FINAL.pdf>
- Hailemariam, A & Erdiaw-Kwasie, M 2022, *Towards a Circular Economy: Implications for Emission Reduction and Environmental Sustainability*, *Business Strategy and the Environment*, vol. 32, <https://doi.org/10.1002/bse.3229>
- Hansson, I & Skogh, G n.d., 'Moral Hazard and Safety Regulation', *The Geneva Papers on Risk and Insurance*, vol. 12, <https://www.jstor.org/stable/41950219>
- Hernantes, J, Maraña, P, Gimenez, R, Sarriegi, J & Labaka, L 2019, 'Towards Resilient Cities: A Maturity Model for Operationalizing Resilience', *Cities*, vol. 84, <https://doi.org/10.1016/j.cities.2018.07.010>
- Heylighen, F & Joslyn, C 2003, *Cybernetics and Second-Order Cybernetics*, Elsevier eBooks, <https://doi.org/10.1016/b0-12-227240-4/00178-7>
- Howell, B & Potgieter, P 2020, 'Politics, Policy and Fixed-line Telecommunications Provision: Insights From Australia', *Telecommunications Policy*, vol. 44, <https://doi.org/10.1016/j.telpol.2020.101999>
- Infrastructure Australia 2019, *An Assessment of Australia's Future Infrastructure Needs*, <https://www.infrastructureaustralia.gov.au/publications/australian-infrastructure-audit-2019>
- International Organization for Standardization 2015, *15288-2023 – ISO/IEC/IEEE International Standard – Systems and software engineering--System life cycle processes*, <https://ieeexplore.ieee.org/document/10123367>
- International Organization for Standardization 2017, *ISO 22316:2017 Security and resilience — Organizational resilience — Principles and attributes*, <https://www.iso.org/standard/50053.html>
- International Organization for Standardization 2018, *Risk Management Guidelines*, International Organization for Standardization, Geneva.
- International Organization for Standardization 2019, *ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements*, <https://www.iso.org/standard/75106.html>
- International Organization for Standardization 2021, *ISO 31000 — Risk Management*, <https://www.iso.org/iso-31000-risk-management.html/>
- International Organization for Standardization and International Electrotechnical Commission 2021, *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks*, <https://www.iso.org/standard/80585.html>
- Internet Association of Australia 2023, *Submission to the Bean Review of the 2023 Optus Outage*, <https://internet.asn.au/wp-content/uploads/2024/01/IAA-Response-to-the-Optus-Outage-TOR-20231222.pdf>
- Kaloudi, N & Li, J 2021, *Comparison of Risk Analysis Approaches for Analyzing Emergent Misbehavior in Autonomous Systems*, Department of Computer Science, Norwegian University of Science and Technology, <https://www.rpsonline.com.sg/proceedings/9789811820168/pdf/213.pdf>
- Kartchner, K 2013, *Consequence Management and National Security*, US eBooks, https://doi.org/10.1057/9781137336439_13

- Kaye, B 2022, *Australia's Optus says up to 10 million customers caught in cyber attack*, Reuters, <https://www.reuters.com/technology/australias-optus-says-up-10-mln-customers-caught-cyber-attack-2022-09-23/>
- King & Wood Mallesons 2024, *Strengthening Australian Critical Infrastructure Against Cyber Risks*, <https://www.kwm.com/au/en/insights/latest-thinking/strengthening-australias-critical-infrastructure-against-cyber-risks-consultation-on-legislative-reforms-close-1-march-2024.html>
- Kozine, I & Andersen, H 2015, *Integration of Resilience Capabilities for Critical Infrastructures Into the Emergency Management Set-up*, Safety and Reliability of Complex Engineered Systems, CRC Press, https://backend.orbit.dtu.dk/ws/files/128948305/Paper_ESREL_2015_postprint.pdf
- KPMG 2023, *70 Percent of Australians Impacted by Natural Disasters*, <https://kpmg.com/au/en/home/media/press-releases/2024/09/70-per-cent-of-australians-impacted-by-natural-disasters.html>
- Kyriakides, Ed & Polycarpou, M 2015, *Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems*, Studies in Computational Intelligence, <https://doi.org/10.1007/978-3-662-44160-2>
- Launius, S 2021, *Evaluation of Comprehensive Taxonomies for Information Technology Threats*, SANS Institute, <https://www.sans.org/white-papers/38360/>
- Lazurko, A, Schweizer, V & Armitage, D 2023, 'Exploring 'Big Picture' Scenarios for Resilience in Social–ecological Systems: Transdisciplinary Cross-impact Balances Modeling in the Red River Basin', *Sustainability Science*, vol. 18, <https://doi.org/10.1007/s11625-023-01308-1>
- Mansouri, M, Nilchiani, R & Mostashari, A 2010, 'A Policy Making Framework for Resilient Port Infrastructure Systems', *Marine Policy*, vol. 34, <https://doi.org/10.1016/j.marpol.2010.03.012>
- Marani, M, Katul, G, Pan, W & Parolari, A 2021, 'Intensity and Frequency of Extreme Novel Epidemics', *Proceedings of the National Academy of Sciences of the United States of America*, vol. 118, <https://doi.org/10.1073/pnas.2105482118>
- McEntire, D & Myers, A 2004, 'Preparing Communities for Disasters: Issues and Processes for Government Readiness', *Disaster Prevention and Management*, vol. 13, <https://doi.org/10.1108/09653560410534289>
- McGillivray, G 2021, *An Expert Explains: How COVID-19 Exposed the Fragility of Global Supply Chains*, World Economic Forum, <https://www.weforum.org/agenda/2021/07/covid-19-pandemic-global-supply-chains/>
- Mentges, A, Halekotte, L, Schneider, M, Demmer T & Lichte, D 2023, 'A Resilience Glossary Shaped by Context: Reviewing Resilience-related Terms for Critical Infrastructures', *International Journal of Disaster Risk Reduction*, vol. 96, <https://doi.org/10.1016/j.ijdrr.2023.103893>
- Monge, P & Contractor, N 2003, *Theories of Communication Networks*, Oxford University Press eBooks, <https://doi.org/10.1093/oso/9780195160369.001.0001>
- Montgomery, D, Polk, T, Ranganathan, M, Souppaya, M, NIST, Barker, W, Dakota Consulting 2020, 'Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD) – Volume B: Approach', *Architecture, and Security Characteristics*, NIST Special Publication 1800-15B, <https://www.nccoe.nist.gov/sites/default/files/legacy-files/iot-ddos-nist-sp1800-15b-draft.pdf>
- Moore, M 2009, *Bridging the Gap: Developing a Tool to Support Local Civilian and Military Disaster Preparedness*, Google Books, https://books.google.com.au/books/about/Bridging_the_Gap.html?id=nZkgAQAAMAAJ&redir_esc=y
- Morrison, S, Fifield, M & Australian Government 2018, *Government Provides 5G Advice to Australian Carriers*, https://parlinfo.aph.gov.au/parlInfo/download/media/pressrel/6164495/upload_binary/6164495.pdf;fileType=application%2Fpdf#search=%22media/pressrel/6164495%22
- Naheed, S 2021, *Understanding Disaster Risk Reduction and Resilience: A Conceptual Framework*, Springer eBooks, https://doi.org/10.1007/978-3-030-61278-8_1
- National Aeronautics and Space Administration (NASA) 2020, *Solar Cycle 25 Is Here. NASA, NOAA Scientists Explain What That Means*, NASA, <https://www.nasa.gov/news-release/solar-cycle-25-is-here-nasa-noaa-scientists-explain-what-that-means/>
- National Emergency Management Agency 2023, *Australian Emergency Management Arrangements Handbook*, https://knowledge.aidr.org.au/media/10162/handbook_aema_web_2023.pdf

- National Resilience Taskforce 2018, *Profiling Australia's Vulnerability: interconnected causes and cascading effects of systemic disaster risk*, Australian Institute for Disaster Resilience, <https://www.aidr.org.au/media/6682/national-resilience-taskforce-profiling-australias-vulnerability.pdf>
- National Telecommunications and Information Administration, The Department of Home Affairs, The Department of Innovation, Science and Economic Development Canada & The Department for Digital, Culture, Media and Sport 2022, *Joint Statement Between the United States of America, Australia, Canada and the United Kingdom on Telecommunications Supplier Diversity*, National Telecommunications and Information Administration, <https://www.ntia.gov/press-release/2022/joint-statement-between-united-states-america-australia-canada-and-united>
- New South Wales Government 2022, *2022 NSW Flood Inquiry*, https://www.nsw.gov.au/sites/default/files/noindex/2022-08/VOLUME_TWO_Full%20report.pdf
- Nguyen, V, Lin, P, Cheng, B, Hwang, R & Lin, Y 2021, 'Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges', *IEEE Communications Surveys and Tutorials*, vol. 23, <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9524814>
- NIST Computer Security Resource Center 2017, *NIST IR 8183 Cybersecurity Framework Manufacturing Profile*, <https://csrc.nist.gov/pubs/ir/8183/upd1/final>
- O'Donnell & K 2013, *Critical Infrastructure Resilience: Resilience Thinking in Australia's Federal Critical Infrastructure Protection Policy*, *SALUS Journal* 1, <https://doaj.org/article/7e6e39b4c93a4913be2001d0850b6a25>
- Optus 2024, *Outage Response*, <https://www.optus.com.au/notices/outage-response>
- Organisation for Economic Development n.d., *Guidelines for Resilience Systems Analysis: How to Analyse Risk and Build a Roadmap to Resilience*, OECD iLibrary, https://www.oecd-ilibrary.org/development/guidelines-for-resilience-systems-analysis-how-to-analyse-risk-and-build-a-roadmap-to-resilience_3b1d3efe-en
- Organisation for Economic Development 2019, *OECD Reviews of Risk Management Policies: Good Governance for Critical Infrastructure Resilience*, OECD iLibrary, <https://www.oecd-ilibrary.org/sites/02f0e5a0-en/index.html?itemId=/content/publication/02f0e5a0-en>
- Osei-Kyei, R, Almeida, L, Ampratwum, G & Tam, V 2022, 'Systematic Review of Critical Infrastructure Resilience Indicators', *Construction Innovation*, vol. 23 no. 5, <https://doi.org/10.1108/ci-03-2021-0047>
- Otter, N & Uschkurat, M 2024, *Conceptual Development of a Resilience Maturity Model for SMEs*, Springer, https://books.google.com.au/books?hl=en&lr=&id=1F38EAAAQBAJ&oi=fnd&pg=PR8&ots=0EFRkKgiCF&sig=Okzfp3fC_UlVaOqF8FZmZtPYICA&redir_esc=y#v=onepage&q&f=false
- Ottosson, M 2022, *Why network intelligence is vital in addressing RAN threats*, Ericsson, <https://www.ericsson.com/en/blog/2022/6/why-network-intelligence-is-vital-in-addressing-ran-threats>
- Patriarca, R, Di Gravio, G, Costantino, F, Falegnami, A & Bilotta, F 2018, 'An Analytic Framework to Assess Organizational Resilience', *Safety and Health at Work*, vol. 9, <https://doi.org/10.1016/j.shaw.2017.10.005>
- Perera, A, Nik, V, Chen, D, Scartezzini, J & Hong, T 2020, 'Quantifying the Impacts of Climate Change and Extreme Climate Events on Energy Systems', *Nature Energy* vol. 5, <https://doi.org/10.1038/s41560-020-0558-0>
- Pescaroli, G & Alexander, D 2016, 'Critical Infrastructure, Panarchies and the Vulnerability Paths of Cascading Disasters', *Natural Hazards*, vol. 82, <https://doi.org/10.1007/s11069-016-2186-3>
- Pescaroli, G & Alexander, D 2018, 'Understanding Compound, Interconnected, Interacting, and Cascading Risks: A Holistic Framework', *Risk Analysis* vol. 38, <https://doi.org/10.1111/risa.13128>
- Phillips, B & Landahl, M 2020, *Business Continuity Planning: Increasing Workplace Resilience to Disasters*, ScienceDirect, <https://doi.org/10.1016/C2017-0-00385-3>
- Prague Cyber Security Conference 2021, *Explore Key Takeaways from Prague Proposals*, <https://www.praguecybersecurityconference.com/prague-proposals/>
- Pursiainen, C & Kytömaa, E 2022, 'From European Critical Infrastructure Protection to the Resilience of European Critical Entities: What Does It Mean', *Sustainable and Resilient Infrastructure*, vol. 8, <https://doi.org/10.1080/23789689.2022.2128562>

Queensland Disaster Management 2023, *Prevention Preparedness Response and Recovery Disaster Management Guideline*, <https://www.disaster.qld.gov.au/disaster-management-guideline>

Queensland Reconstruction Authority 2024, *2023-24 South Queensland Severe Storms*, <https://www.qra.qld.gov.au/2023-24-South-Queensland-Severe-Storms>

Queensland Reconstruction Authority 2024, *Tropical Cyclone Kirrily: the northern system that became a statewide disaster event*, <https://www.qra.qld.gov.au/news-case-studies/case-studies/tropical-cyclone-kirrily-northern-system-became-statewide-disaster-event>

Rathnayaka, B, Siriwardana, C, Robert, D, Amaratunga, D & Setunge, S 2022, 'Improving the Resilience of Critical Infrastructures: Evidence-based Insights From a Systematic Literature Review', *International Journal of Disaster Risk Reduction*, vol. 78, <https://doi.org/10.1016/j.ijdr.2022.103123>

Rinaldi, S, Peerenboom, J & Kelly, T 2001, 'Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies', *IEEE Control Systems*, vol. 21, <https://doi.org/10.1109/37.969131>

Rocher, L, Hendrickx, J & Montjoye, Y 2019, 'Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models', *Nature Communications*, vol. 10, <https://doi.org/10.1038/s41467-019-10933-3>

Ronan, K, Haynes, K, Amri, A, Towers, B, Alisic, E, Davie, S, Ireland, N & Petal, M n.d., *Child-centred disaster risk reduction: can disaster resilience programs reduce risk and increase the resilience of children and households?*, Australian Disaster Resilience Knowledge Hub, <https://knowledge.aidr.org.au/resources/ajem-jul-2016-child-centred-disaster-risk-reduction-can-disaster-resilience-programs-reduce-risk-and-increase-the-resilience-of-children-and-households/>

Ross, R, Pillitteri, V, Graubart, R, Bodeau, B & McQuaid, R 2021, *Developing Cyber-Resilient Systems: A Systems Engineering Approach*, National Institute of Standards and Technology, <https://doi.org/10.6028/nist.sp.800-160v2r1>

Roy Morgan 2022, *A Majority of Australians Have No Trust in Telcos*, <https://www.roymorgan.com/findings/a-majority-of-australians-have-no-trust-in-telcos>

Senate Economics Reference Committee 2017, *2016 Census: issues of trust*, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/2016Census/Report

Senate Select Committee on Australia's Disaster Resilience 2023, *Interim Report*, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Disaster_Resilience/DisasterResilience/Interim_Report

Senate Select Committee on Foreign Interference through Social Media 2023, *Final Report of the Select Committee on Foreign Interference Through Social Media*, https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/pubs/rp/rp2324/Quick_Guides/ForeignInterferencethroughSocialMedia

Shaked, A, Tabansky, L & Reich Y 2020, 'Incorporating Systems Thinking Into a Cyber Resilience Maturity Model', *IEEE Journals & Magazine* vol. 1, <https://ieeexplore.ieee.org/document/9302574>

Singh, P, Amekudzi-Kennedy, A, Ashuri, B, Chester, M, Labi, S & Wall, T 2022, *Developing Adaptive Resilience in Infrastructure Systems: An Approach to Quantify Long-term Benefits*, Sustainable and Resilient Infrastructure 8, <https://doi.org/10.1080/23789689.2022.2126631>

Slezak, M & Bogle, A 2018, *Huawei Banned From 5G Mobile Infrastructure Rollout in Australia*, ABC News, <https://www.abc.net.au/news/2018-08-23/huawei-banned-from-providing-5g-mobile-technology-australia/10155438>

Sonesson, T, Johansson, J & Cedergren, A 2021, 'Governance and Interdependencies of Critical Infrastructures: Exploring Mechanisms for Cross-sector Resilience', *Safety Science*, vol. 142, <https://doi.org/10.1016/j.ssci.2021.105383>

Steen, R, Haug, O & Patriarca R, 2023, 'Business Continuity and Resilience Management: A Conceptual Framework', *Journal of Contingencies and Crisis Management*, vol. 32, <https://doi.org/10.1111/1468-5973.12501>

Su, W & Junge, S 2023, 'Unlocking the Recipe for Organizational Resilience: A Review and Future Research Directions', *European Management Journal*, vol. 41, <https://doi.org/10.1016/j.emj.2023.03.002>

Svegrup, L, Johansson, J & Hassel, H 2019, *Integration of Critical Infrastructure and Societal Consequence Models: Impact on Swedish Power System Mitigation Decisions*, Risk Analysis, vol. 39, <https://doi.org/10.1111/risa.13272>

Tarala, J, Tarala, K & Enclave Security 2015, *Open Threat Taxonomy*, Enclave Security, https://www.auditscripts.com/resources/open_threat_taxonomy_v1.1a.pdf

Telstra Corporation Limited 2011, *Submission to Public inquiry to make final access determinations for the declared fixed line services*, <https://www.accc.gov.au/system/files/Schedule%20A.3%20of%20Telstra%20public%20submission.pdf>

The Cybersecurity and Infrastructure Security Agency, National Security Agency, Federal Bureau of Investigation, Australian Signals Directorate's Australian Cyber Security Centre, Canadian Centre for Cyber Security, New Zealand National Cyber Security Centre, Computer Emergency Response Team New Zealand, & National Cyber Security Centre 2023, *2022 Top Routinely Exploited Vulnerabilities*, Cybersecurity and Infrastructure Security Agency, <https://www.cisa.gov/news-events/alerts/2023/08/03/cisa-nsa-fbi-and-international-partners-release-joint-csa-top-routinely-exploited-vulnerabilities>

The European Space Agency 2024, *The May 2024 Solar Storm: Your Questions Answered*, ESA, https://www.esa.int/Space_Safety/Space_weather/The_May_2024_solar_storm_your_questions_answered

Thomas, J, McCosker, A, Parkinson, S, Hegarty, K, Featherstone, D, Kennedy, J, Holcombe-James, I, Ormond-Parker L, & Ganley 2023, *Measuring Australia's Digital Divide: Australian Digital Inclusion Index: 2023*, ARC Centre of Excellence for Automated Decision-Making and Society, RMIT University, Swinburne University of Technology & Telstra, <https://doi.org/10.25916/528s-ny91>

Tippet, H 2024, *Victoria's power outage caught thousands by surprise — here's how it happened*, ABC News, <https://www.abc.net.au/news/2024-02-14/victoria-melbourne-power-outage-storms-how-did-it-happen/103464714>

Ungar, M 2018, 'Systemic Resilience: Principles and Processes for a Science of Change in Contexts of Adversity Principles and Processes for a Science of Change in Contexts of Adversity', *Ecology and Society* vol. 23, <https://www.jstor.org/stable/26796886>

United Nations Office for Disaster Risk Reduction 2021, *Principles for Resilient Infrastructure*, <https://www.undrr.org/publication/principles-resilient-infrastructure>

United Nations Office for Disaster Risk Reduction 2007, *Vulnerability*, Sendai Framework Terminology on Disaster Risk Reduction, <https://www.undrr.org/terminology/vulnerability>

United Nations System Chief Executives Board for Coordination n.d., *UN Organizational Resilience Maturity Model*, Addison-Wesley Professional, <https://unsceb.org/sites/default/files/2021-12/Approved%20Organizational%20Resilience%20Maturity%20Model.pdf>

United States Department of State 2021, *The Clean Network – United States Department of State*, <https://2017-2021.state.gov/the-clean-network/>

Vivian, S & Bardon, J 2024, *ADF has airlifted 380 Borroloola residents to Darwin as McArthur River hits flood peak*, ABC News, <https://www.abc.net.au/news/2024-03-22/borroloola-flood-mcarthur-river-adf-evacuation/103619244>

Ward, P, Daniell, J, Duncan, M, Dunne, A, Hananel, C, Hochrainer-Stigler, S & Tijssen, A 2022, *Invited Perspectives: A Research Agenda Towards Disaster Risk Management Pathways in Multi-(Hazard-)Risk Assessment, Natural Hazards and Earth System Sciences*, vol. 22, <https://doi.org/10.5194/nhess-22-1487-2022>

Weule, G 2022, *Just How Bad Could a Big Solar Storm Be in the Internet Age? And How Would Australia Be Affected?*, ABC News, <https://www.abc.net.au/news/science/2022-03-01/solar-storm-risks-power-network-internet/100812978>

Wirtz, J 2013, *What Just Happened? Situational Awareness, Threat Characterization, and Effective Consequence Management*, Palgrave Macmillan US eBooks, https://doi.org/10.1057/9781137336439_2

World Economic Forum 2024, *Global Risks Report 2024*, <https://www.weforum.org/publications/global-risks-report-2024/in-full/global-risks-2034-over-the-limit/>

Yang, Z, Barroca, B, Laffréchine, B, Weppe, A, Bony-Dandrieux, A & Daclin, N 2023, 'A Multi-criteria Framework for Critical Infrastructure Systems Resilience', *International Journal of Critical Infrastructure Protection*, vol. 42, <https://doi.org/10.1016/j.ijcip.2023.100616>



Australian
National
University



TECH POLICY
DESIGN CENTRE

Tech Policy Design Centre

Australian National University

E: techpolicydesign@anu.edu.au

W: www.techpolicydesign.au

in Tech Policy Design Centre