

Digital Recovery

Considerations for Recovery Governance, Planning and Operations

Foreword

Over recent years, I have had the privilege of working alongside communities, local authorities, iwi, government agencies, infrastructure providers and recovery practitioners before, during and after emergencies. Across each event, the circumstances have differed, but one observation has remained remarkably consistent.

Recovery is becoming increasingly digital.

Not because technology has become more important than people, but because people now rely upon digital capability to communicate with whānau, access essential services, make decisions, reconnect businesses, restore livelihoods and participate in their communities. Likewise, the organisations responsible for supporting recovery increasingly depend upon digital information, communications, geospatial intelligence and interconnected systems to understand impacts, coordinate activities and support informed decision-making.

Yet despite this growing dependence, digital recovery has received relatively little attention as a distinct area of recovery practice.

This paper was not written from a technology perspective. Nor is it intended to redefine existing recovery doctrine. Rather, it emerged from a series of observations made through emergency management practice, governance and conversations with colleagues across multiple sectors. Collectively, those observations suggest that while our understanding of recovery continues to evolve, our thinking about digital capability has not always evolved alongside it.

The purpose of this paper is therefore not to provide definitive answers. Instead, it seeks to begin a conversation.

It explores how digital capability increasingly enables every recovery environment and proposes that recovery planning may benefit from recognising digital capability not as another recovery environment, but as a foundational condition that supports recovery across them all. It introduces several concepts intended to stimulate discussion, including Digital Intelligence, the Digital Recovery Stack and Digital Recovery Maturity, while acknowledging that these ideas will continue to evolve through practice, collaboration and shared learning.

Canterbury has a long history of innovation in emergency management and recovery. It is my hope that this paper contributes, in some small way, to that tradition by encouraging discussion about how recovery planning can continue to adapt as our communities, infrastructure and society become increasingly interconnected.

If this paper encourages new conversations, new partnerships or even new questions, then it will have achieved its purpose.

Elle Archer
CDEM Recovery Canterbury
20 July 2026

Table of Contents

Digital Recovery	1
Considerations for Recovery Governance, Planning and Operations.....	1
Foreword.....	1
1. Introduction	3
2. Digital as Critical Infrastructure	4
3. The Digital Recovery Stack.....	6
4. Digital Intelligence Across the Recovery Continuum.....	7
5. Governance Considerations for Digital Recovery.....	9
Governance Considerations	11
6. Digital Recovery Maturity	11
7. A Call to Action.....	13
Overall Reflection	15

1. Introduction

Recovery is ultimately about people, communities and the systems that enable them to live, work and participate in society. While disasters have traditionally been viewed through their impacts on the social, built, economic and natural environments, the increasing digitisation of modern society means that nearly every aspect of recovery now depends, to some degree, on digital capability.

In Aotearoa New Zealand, communities are increasingly connected through digital services that underpin government, emergency management, healthcare, education, banking, commerce and community life. Communities rely on these systems to communicate with whānau, access essential services, reconnect businesses, restore education, coordinate volunteers, process insurance claims, access welfare support and make informed decisions throughout recovery. Likewise, organisations responsible for recovery depend upon digital information, communications, geospatial intelligence, cloud services, operational systems and data to understand impacts, prioritise resources and coordinate recovery activities across multiple agencies and jurisdictions. Recent emergencies, together with increasing cyber activity and the growing complexity of critical infrastructure, have demonstrated that digital capability is now an essential consideration for contemporary recovery planning.

Digital capability has therefore evolved beyond being viewed solely as an organisational support function. It has become a foundational enabler of modern society and, increasingly, a critical dependency for the successful recovery of every recovery environment.

Historically, recovery planning has largely focused on repairing physical infrastructure and restoring community services following natural hazards. While these remain fundamental, the environments in which recovery now occurs are increasingly characterised by interconnected digital systems, globally distributed technology platforms, complex supply chains and rapidly evolving cyber threats. Recovery may follow physical disasters, digital disruption, or a combination of both. In many cases, digital disruption may continue throughout the recovery process, requiring communities and organisations to recover while simultaneously managing ongoing technological, cyber and information-related challenges.

As emergency management continues to evolve nationally, there is an increasing opportunity to strengthen how digital capability is considered across the wider emergency management system. While significant progress has been made in developing nationally consistent approaches to preparedness, response and recovery, the growing dependence on digital systems presents an opportunity to further integrate digital capability into recovery governance, planning and operations.

This paper explores the role of digital recovery within emergency management and identifies the key governance, planning and operational considerations necessary to support recovery at local, regional and national levels. It proposes that digital recovery should not be considered as a separate recovery environment, but as a foundational capability that enables recovery across the social, built, economic and natural environments. It introduces the concept of *Digital Recovery Maturity* as a means of supporting future capability development and outlines the foundations of a *Canterbury Digital Recovery Framework* that may contribute to broader national conversations.

As New Zealand continues to increase its reliance on digital systems, the question is no longer whether digital capability is critical to recovery. The question is whether our recovery planning has evolved sufficiently to recognise that dependence.

2. Digital as Critical Infrastructure

For many years, critical infrastructure has been understood as the physical assets and services essential to the functioning of society. Electricity, water, wastewater, transport, fuel and telecommunications have traditionally formed the foundation of emergency management planning because prolonged disruption to these services has significant consequences for public safety, economic activity and community wellbeing.

Increasingly, however, these sectors are themselves dependent upon digital systems.

Electricity networks rely on digital monitoring and control systems. Water treatment and distribution systems are managed through automated operational technologies. Emergency services depend upon digital communications, geospatial information and shared situational awareness. Banking, insurance, health, education, logistics and government services all rely upon interconnected digital platforms to deliver essential services to communities.

Digital capability is therefore no longer simply supporting critical infrastructure. It has become integral to how critical infrastructure operates, enabling the continuity, coordination and resilience of essential services across multiple sectors.

This increasing interdependence presents an opportunity to broaden how recovery planning considers critical infrastructure. Rather than viewing digital systems solely as enabling technologies, recovery planning should recognise that the resilience of physical infrastructure and digital capability are now fundamentally interconnected. The restoration of one increasingly depends upon the restoration of the other.

This evolution also has important implications for lifeline utilities. Electricity, water, wastewater, transport, fuel and telecommunications all rely upon digital systems to monitor, control, coordinate and restore essential services. As these interdependencies continue to grow, digital capability should be recognised as a fundamental component of lifeline resilience and recovery planning, rather than as a separate supporting function.

Recognising digital capability in this way does not redefine critical infrastructure. Rather, it acknowledges that the systems supporting modern communities have evolved, and that recovery planning must evolve alongside them.

The implications for recovery are significant.

The restoration of physical infrastructure alone no longer guarantees the restoration of essential services. A repaired building may remain unusable without connectivity. A restored water treatment plant may remain constrained if operational control systems are unavailable. Healthcare facilities, welfare services, financial institutions and local authorities may have functioning premises while remaining unable to operate effectively if critical digital systems, data or communications have not been restored.

The increasing interdependence between physical and digital infrastructure also changes the nature of disruption. Damage to physical assets may interrupt digital services, while disruption to digital systems may significantly reduce the ability to manage, monitor or restore physical infrastructure. Recovery planning must therefore recognise that physical and digital recovery are increasingly inseparable.

This interdependence extends beyond infrastructure operators. Communities themselves now depend on digital capability to reconnect with whānau, access trusted information, communicate with emergency services, engage with employers, continue education, manage finances, access government support and participate in community recovery. Digital exclusion, whether caused by infrastructure failure, cyber disruption or unequal access, has the potential to slow recovery and increase existing social and economic inequities.

Alongside this increasing dependence, the operating environment has also become more complex. Digital infrastructure now exists within a globally connected ecosystem where cybercrime, organised criminal networks, state-sponsored actors, supply chain vulnerabilities and rapidly evolving technologies present an ongoing challenge to resilience. While the causes of disruption may differ from those associated with natural hazards, the consequences for communities can be equally significant. Recovery planning should therefore recognise that digital disruption may occur independently, alongside, or as a consequence of other emergencies.

Recognising digital capability as critical infrastructure is not intended to elevate technology above other recovery priorities. Rather, it acknowledges that digital capability has become one of the foundational conditions upon which modern communities, essential services and recovery itself now depend.

Figure 1. Digital dependency across critical infrastructure

Critical Infrastructure	Increasing Digital Dependency
Electricity	Network monitoring, SCADA, demand management, outage management, customer communications
Water and Wastewater	Treatment automation, telemetry, asset monitoring, operational control
Transport	Traffic management, signalling, logistics, navigation, public information
Telecommunications	Core networks, cloud services, software-defined infrastructure, satellite integration
Health	Electronic health records, diagnostics, pharmacy systems, telehealth
Banking and Finance	Payments, banking platforms, digital identity, fraud detection
Government Services	Customer services, welfare systems, planning, regulatory services, emergency management
Emergency Management	Intelligence, GIS, communications, resource management, public information, coordination

3. The Digital Recovery Stack

The increasing importance of digital recovery is not simply a consequence of technology becoming more widespread. It reflects the growing interdependence between physical infrastructure, digital capability and the communities they serve.

Traditional recovery planning has often considered infrastructure, services and communities as separate systems that are restored independently. Increasingly, however, these systems operate as an interconnected network, where disruption to one layer can rapidly affect many others. Digital capability now acts as the connective layer between physical infrastructure, essential services and community recovery.

This relationship can be viewed as a *Digital Recovery Stack*.

Figure 2. The Digital Recovery Stack



Each layer supports the one above it.

Physical infrastructure provides the foundation upon which digital infrastructure operates. Digital infrastructure enables the delivery of digital services and access to trusted information. Those services generate the intelligence required to support informed decision-making throughout recovery. Ultimately, effective recovery depends upon restoring community confidence, participation and trust.

Failure within any layer has the potential to affect every layer above it.

For example, widespread power outages may interrupt telecommunications, resulting in the loss of internet connectivity, cloud services and operational systems. This may limit access to banking, healthcare, education, emergency information and government services, reducing the ability of communities to make informed decisions and participate in recovery.

Conversely, digital disruption may occur while physical infrastructure remains largely intact. Cyber incidents, software failures, telecommunications outages or cloud service disruptions may significantly impair the delivery of essential services despite there being little or no physical damage. Communities may experience similar recovery challenges regardless of whether the initial disruption originated from a natural hazard, technology failure or malicious activity.

This increasing interdependence reinforces the need to consider digital recovery as a strategic capability rather than solely an information technology function. Recovery planning should recognise that restoring digital capability is not simply about reconnecting systems. It is about restoring the conditions necessary for communities, organisations and governments to make decisions, deliver services and rebuild confidence.

Importantly, the Digital Recovery Stack should not be interpreted as a rigid hierarchy. Recovery rarely progresses sequentially from one layer to the next. Activities occur simultaneously, often requiring decisions to be made with incomplete information while services continue to be restored. The model is intended to illustrate the relationships between the layers of recovery rather than prescribe the order in which recovery occurs.

As digital dependence continues to increase, understanding these relationships becomes increasingly important for governance groups responsible for setting priorities, allocating resources and overseeing long-term recovery. Decisions made within one part of the system are increasingly likely to influence outcomes across many others.

Observation

The objective of digital recovery is not to restore technology for its own sake. Its purpose is to restore the digital conditions that enable people, communities, organisations and governments to recover together.

4. Digital Intelligence Across the Recovery Continuum

Digital recovery extends beyond restoring infrastructure, systems and services. It also depends upon the ability to understand what has happened, anticipate what may occur next and make informed decisions throughout the recovery process. This requires more than access to information. It requires digital intelligence.

For the purposes of recovery, digital intelligence can be understood as the ability to transform digital information into shared understanding that supports coordinated decision-making before, during and after an event. It brings together information from multiple sources, provides context, identifies emerging patterns and enables decision-makers to prioritise actions, allocate resources and monitor recovery over time.

As communities become increasingly connected, the volume, diversity and velocity of digital information continues to increase. Remote sensors, satellite imagery, geospatial information systems, operational technologies, telecommunications networks, infrastructure monitoring,

social media, community reporting, financial systems and numerous other digital platforms all contribute to an increasingly rich picture of an event and its consequences. Individually these systems provide data. Collectively they have the potential to provide intelligence.

The value of digital intelligence is realised when information is integrated across organisations and recovery environments to develop a common understanding of impacts, needs, priorities and progress. This shared understanding enables governance groups, recovery managers, operational agencies, infrastructure providers, iwi, community organisations and central government to make decisions based on a common picture rather than isolated information.

Importantly, digital intelligence is not confined to the response phase of an emergency. It supports every phase of emergency management and becomes increasingly valuable as recovery progresses.

During readiness, digital intelligence assists organisations to understand critical dependencies, identify vulnerabilities, map digital infrastructure and strengthen resilience before an event occurs.

During response, digital intelligence contributes to situational awareness, supports consequence assessment, informs operational priorities and assists with the coordination of resources across agencies.

During recovery, digital intelligence supports impact assessments, funding decisions, infrastructure restoration, community engagement, welfare planning, economic recovery, environmental monitoring and the ongoing measurement of recovery outcomes. As recovery transitions into business-as-usual, digital intelligence also provides the evidence required to evaluate recovery activities, capture lessons identified and strengthen future preparedness.

The growing dependence on digital intelligence also introduces new considerations for recovery planning. Information must remain trusted, available and accessible. Data integrity becomes as important as data availability. Organisations must be able to validate information, manage misinformation and disinformation, protect privacy, maintain cyber security and continue operating when digital systems are degraded or unavailable.

The operating environment must also be recognised as increasingly contested. Cyber crime, organised criminal networks, state-sponsored actors and other malicious actors continue to develop increasingly sophisticated capabilities designed to exploit vulnerabilities within digital systems, supply chains and critical infrastructure. Recovery planning should therefore assume that digital disruption may continue during recovery and that cyber security, digital resilience and trusted information are fundamental components of successful recovery.

Digital intelligence is therefore more than an information management capability. It is a strategic recovery capability. It provides the shared understanding that enables communities, organisations and governments to navigate complexity, coordinate recovery activities and make confident decisions throughout the recovery journey.

Recovery decisions are only as effective as the quality of the information upon which they are based. As digital dependence increases, digital intelligence becomes not simply an operational capability, but a governance capability.

Figure 3. Digital Intelligence Across the Four Rs

Phase	Role of Digital Intelligence
Reduction	Identify vulnerabilities, understand interdependencies, monitor risks, inform investment decisions and strengthen resilience.
Readiness	Map critical digital infrastructure, establish data sharing arrangements, develop common operating pictures, exercise digital recovery arrangements and identify capability gaps.
Response	Support situational awareness, consequence assessment, intelligence products, operational coordination, resource allocation and public information.
Recovery	Monitor impacts, prioritise recovery activities, support governance decisions, coordinate agencies, track recovery outcomes, identify emerging risks and capture lessons for future resilience.

Observation

Digital information becomes valuable when it creates shared understanding. Shared understanding enables coordinated decision-making. Coordinated decision-making enables recovery.

5. Governance Considerations for Digital Recovery

As digital capability becomes increasingly fundamental to community recovery, governance arrangements must evolve alongside it. Digital recovery is not solely an operational or technical responsibility. It requires strategic oversight to ensure that decisions relating to investment, prioritisation, risk, partnerships and long-term resilience are made in the interests of communities and the systems upon which they depend.

Unlike many physical assets, digital systems are often highly interconnected across organisations, sectors and jurisdictions. Critical services may rely upon infrastructure owned by multiple providers, cloud platforms hosted offshore, shared digital services, third-party vendors and nationally managed systems. Recovery decisions made within one organisation may therefore have consequences for many others.

Governance arrangements should recognise these interdependencies and provide mechanisms to support coordinated decision-making across local authorities, infrastructure providers, emergency management agencies, iwi, central government, private sector partners and community organisations.

Digital recovery also requires a broader understanding of risk. While natural hazards continue to present significant challenges, governance groups should recognise that recovery may occur in an environment where cyber incidents, malicious actors, misinformation, supply chain disruption or technology failures continue to influence decision-making. Recovery planning should therefore consider both the restoration of digital capability and the resilience of digital systems throughout the recovery process.

Importantly, governance is not responsible for managing technology. It is responsible for ensuring that the conditions exist for effective recovery.

This includes understanding where critical digital dependencies exist, recognising systemic risks, ensuring appropriate investment decisions are made, supporting collaboration across organisations and maintaining public confidence throughout recovery.

As communities become increasingly dependent upon digital services, governance also has an important role in ensuring recovery remains equitable. Not all communities experience digital disruption equally. Differences in connectivity, digital literacy, affordability, accessibility and trust may influence an individual's ability to access information, government services, financial assistance and community support. Recovery planning should therefore seek to reduce digital inequity rather than unintentionally reinforcing existing disadvantage.

Governance also has an important stewardship role. Decisions made during recovery will influence the resilience of communities for many years beyond the event itself. Where opportunities exist, recovery should seek not only to restore digital capability, but to strengthen resilience, improve interoperability, reduce systemic vulnerabilities and build greater adaptive capacity for future emergencies.

Ultimately, digital recovery is not governed through technology alone. It is governed through leadership, collaboration and informed decision-making.

Digital recovery should not be considered in isolation from existing regional and national resilience initiatives. Rather, it complements established work relating to lifeline utilities, infrastructure resilience, emergency management capability, business continuity, cyber security and critical infrastructure protection by considering how these capabilities collectively enable community recovery.

Governance Considerations

Governance groups may wish to consider the following questions when planning for, overseeing or reviewing digital recovery.

Figure 4. Governance Considerations

Governance Theme	Considerations
Critical Dependencies	What essential community services depend upon digital capability? Where are the key interdependencies between organisations, infrastructure and technology?
Digital Intelligence	Do decision-makers have access to trusted, timely and shared information throughout recovery?
Cyber Resilience	Can recovery continue if digital systems remain compromised or subject to ongoing malicious activity?
Roles and Responsibilities	Are governance, operational and technical responsibilities clearly understood across agencies?
Partnerships	How will local authorities, iwi, infrastructure providers, central government and the private sector coordinate digital recovery?
Digital Equity	Which communities may face barriers accessing digital services during recovery, and how will these be addressed?
Information Integrity	How will trusted information be maintained while managing misinformation, disinformation and cyber threats?
Investment	Does recovery create opportunities to improve resilience rather than simply replace what previously existed?
Capability	Does the region have sufficient digital capability, specialist expertise and surge capacity to support prolonged recovery?
Stewardship	How do today's recovery decisions strengthen long-term community resilience and future preparedness?

Observation

Digital recovery is not governed through technology. It is governed through the decisions people make about technology.

6. Digital Recovery Maturity

Recovery is not simply measured by the restoration of technology. Successful digital recovery reflects an organisation's ability to restore essential services, support informed decision-making, maintain public confidence and strengthen resilience for the future.

As communities become increasingly dependent upon digital capability, recovery planning must also mature. This requires moving beyond a focus on restoring individual systems towards

developing an integrated understanding of how digital capability supports communities, critical infrastructure and long-term recovery outcomes.

The concept of *Digital Recovery Maturity* provides a way of thinking about this progression. Rather than representing a compliance framework, it describes the evolution of capability as organisations move from restoring technology towards embedding digital resilience across recovery planning, governance and operations.

The maturity model recognises that recovery is not complete when systems are switched back on. Recovery is complete when digital capability once again enables communities, organisations and governments to function with confidence, while being better prepared for future disruption.

Figure 5. Digital Recovery Maturity

Level	Description	Recovery Focus
Level 1 – Restore Connectivity	Essential communications and critical digital infrastructure are re-established to enable immediate community and organisational functions.	Restore access.
Level 2 – Restore Essential Services	Priority digital services, operational systems and critical information are restored to support the delivery of essential community services.	Restore services.
Level 3 – Restore Community Capability	Communities, businesses and organisations regain the ability to participate effectively in social, economic and civic life through trusted digital capability.	Restore participation.
Level 4 – Restore Confidence	Digital systems are trusted, information is reliable, governance is informed and communities have confidence in the integrity, security and availability of digital services.	Restore trust.
Level 5 – Build Future Resilience	Recovery investments strengthen digital resilience, reduce systemic vulnerabilities, improve interoperability and enhance preparedness for future emergencies.	Build back stronger.

This progression reflects an important shift in thinking. Digital recovery is not simply an information technology activity undertaken after an event. It is a strategic investment in the future resilience of communities.

Reaching higher levels of digital recovery maturity requires collaboration across multiple sectors. Local government, central government, iwi, infrastructure providers, emergency management agencies, community organisations, research institutions and the private sector each contribute unique capability and expertise. No single organisation owns digital recovery. It is a shared responsibility requiring coordinated leadership and collective stewardship.

Importantly, maturity does not necessarily correlate with organisational size or investment. Smaller communities with strong relationships, well understood digital dependencies, effective

governance and trusted partnerships may demonstrate greater digital recovery capability than larger organisations with more complex but fragmented systems. Maturity is therefore as much about leadership, coordination and shared understanding as it is about technology.

As the digital landscape continues to evolve, so too will the challenges facing recovery. Artificial intelligence, increasingly sophisticated cyber threats, quantum technologies, greater reliance on cloud services and expanding global interdependencies will continue to reshape how communities prepare for, respond to and recover from emergencies. Recovery planning must therefore remain adaptive, recognising that digital capability is not static, but an evolving component of community resilience.

Developing digital recovery maturity is ultimately an investment in people. Technology provides the capability, but communities, organisations and leaders determine how that capability is used to support recovery. The objective is not simply to recover from disruption, but to create the conditions in which future recovery becomes faster, more coordinated and more resilient.

Observation

Digital recovery reaches maturity when communities no longer view digital capability as technology, but as an essential condition for participation, resilience and recovery.

7. A Call to Action

The increasing dependence of communities, organisations and critical infrastructure on digital capability presents an opportunity to strengthen recovery planning across the Canterbury region and contribute to the ongoing development of national recovery capability.

The following recommendations are intended to support future discussion within the Regional Recovery Advisory Governance Group and inform the continued evolution of recovery planning at local, regional and national levels.

Recommendation 1

Recognise digital capability as a foundational enabler of recovery.

Digital capability should be recognised as a cross-cutting enabler that supports recovery across the social, built, economic and natural environments. Rather than being considered solely as an information technology function, digital capability should be incorporated into recovery governance, planning and operational arrangements as an essential condition for community recovery.

Recommendation 2

Develop a Canterbury Digital Recovery Framework.

Building on the observations and considerations outlined in this paper, Canterbury should develop a practical Digital Recovery Framework that supports Recovery Managers, governance groups and partner agencies before, during and after emergencies.

The framework should provide guidance on digital recovery governance, digital intelligence, critical digital infrastructure, partnerships, capability development and regional coordination. It should be designed to complement existing recovery doctrine rather than duplicate it.

Recommendation 3

Embed digital intelligence throughout the recovery continuum.

Digital intelligence should be recognised as a strategic capability that supports decision-making throughout reduction, readiness, response and recovery.

Future recovery planning should strengthen the integration of geospatial information, consequence assessment, infrastructure intelligence, community information, digital monitoring and recovery evaluation to improve shared understanding and support evidence-based decision-making.

Recommendation 4

Strengthen regional understanding of critical digital infrastructure and interdependencies.

A regional assessment should be undertaken to better understand the digital systems, services and dependencies that enable essential community functions.

This should include consideration of:

- critical digital infrastructure and supporting technologies
- dependencies between infrastructure sectors
- cloud services and third-party providers
- digital identity and authentication services
- cyber resilience
- digital supply chains
- regional capability and surge capacity
- potential single points of failure
- alternative communications and continuity arrangements.

Improving visibility of these interdependencies will strengthen both preparedness and recovery planning.

Recommendation 5

Build regional digital recovery capability and maturity.

Digital recovery capability should become an ongoing component of recovery readiness.

This should include:

- incorporating digital recovery into regional exercises
- strengthening governance capability
- developing guidance for Recovery Managers

- improving collaboration between local government, infrastructure providers, iwi, central government, research organisations, and the private sector
- identifying future capability requirements associated with emerging technologies, including artificial intelligence and quantum computing
- contributing lessons and emerging practice to future guidance developed across the emergency management system

Developing capability before an event occurs will improve the region's ability to recover from both physical and digital disruption.

Overall Reflection

Recovery has always adapted to reflect the society it serves.

As communities have evolved, so too have the systems that sustain them.

Today, digital capability underpins communication, critical infrastructure, public services, commerce, governance and community participation. Increasingly, it underpins recovery itself. It enables organisations to understand events, coordinate recovery activities and support informed decision-making across every stage of the recovery journey.

This paper proposes that digital recovery should no longer be viewed as a specialist technical activity undertaken by information technology professionals. It is a shared responsibility that extends across governance, planning, operations and community leadership.

Recognising digital capability as a foundational enabler of recovery represents an important evolution in recovery thinking. It acknowledges that restoring technology is not the objective. The objective is to restore the digital conditions that enable people, communities, organisations and governments to recover together.

As Aotearoa New Zealand continues to strengthen its national resilience, there is an opportunity to ensure that digital recovery becomes an integral part of future recovery planning. Canterbury is well placed to contribute to this conversation through practical experience, collaborative leadership and a commitment to continual learning.

The development of a Canterbury Digital Recovery Framework offers one pathway towards that future. While this paper does not seek to provide all of the answers, it aims to begin a conversation that will become increasingly important as digital capability continues to shape the way communities prepare for, respond to and recover from emergencies.

Digital recovery does not replace existing recovery practice. It provides another lens through which recovery can be understood. It recognises that the systems supporting modern communities have evolved, and that recovery planning must evolve with them.

Recovery has traditionally focused on restoring what was damaged.

Digital recovery asks a different question. *What conditions must exist for society to recover?*

Increasingly, one of those conditions is digital capability.

This paper is intended to stimulate discussion and support the continued evolution of digital recovery thinking across Canterbury and Aotearoa New Zealand.