NSW Critical Infrastructure Resilience Strategy

Partner, Prepare, Provide

NSW Department of Justice | Office of Emergency Management

Copyright

Office of Emergency Management
GPO Box 5434
SYDNEY NSW 2001
(02) 9212 9200

Acknowledgements

Acknowledgements: The contributions made by all the stakeholders involved in the planning, workshops, and development of the NSW Critical Infrastructure Resilience Strategy 2018 are acknowledged.

Disclaimer

This document has been prepared by the Department of Justice for general information purposes and while every care has been taken in relation to its accuracy, no warranty is given or implied. Further, recipients should obtain their own independent advice before making any decisions that rely on this information.

Table of Contents

Ministerial Foreword

Critical infrastructure (CI) is vital to the social wellbeing, economic prosperity, and environmental values of the people of New South Wales (NSW).

NSW benefits from infrastructure that provides secure and reliable critical services, such as food, water, electricity, telecommunications and health care. To continue to enjoy these benefits, the risks to critical infrastructure must be managed through an all-hazards approach. This includes mitigating and planning for emergencies resulting from natural (e.g. bushfire, storms, and floods), technological (e.g. cyberattack) and malicious (e.g. terrorism) hazards. Increasing the resilience of critical infrastructure also increases the community's ability to withstand and recover from these events.

The *NSW Critical Infrastructure Resilience Strategy 2018* complements recommendations within the *2017 State Level Emergency Risk Assessment* and the *NSW State Infrastructure Strategy 2018-2038*. It builds on previous work including the Commonwealth's *2015 Critical Infrastructure Resilience Strategy* and COAG's *National Strategy for Disaster Resilience*.

This strategy is the result of a collaborative partnership between government, the NSW community, and infrastructure owners and operators. A dedicated working group, established by the State Emergency Management Committee, has coordinated a discussion paper and industry consultation sessions to produce this five-year strategy. It demonstrates the commitment of all parties to work together to build a strong and resilient NSW that can withstand, adapt and thrive when threatened by emergencies.

NSW infrastructure needs to withstand the shocks of natural, technological, and malicious hazards to continue operating, be returned to service as soon as possible after any service disruption, and address long-term stresses such as climate change and population growth.

The outcomes, priorities, and key initiatives of this strategy are designed to create benefits for infrastructure providers, all levels of government, and importantly, the people and businesses of NSW.

The strategy will be supplemented with user resources, to provide infrastructure, planning, and emergency services professionals with tools and techniques to improve critical infrastructure resilience across NSW.

Today, we are planning and building the infrastructure we will be using in 2050, in what will be a very different climate and a very different New South Wales. We must integrate resilience into today's infrastructure to provide for tomorrow's prosperity.

Your support of the NSW Critical Infrastructure Resilience Strategy will lead to a safer, more secure, and more disaster resilient NSW.

Signed,

Troy Grant

Minister for Emergency Services

The NSW Emergency Management and Disaster Resilience Review

In August 2016 the State Emergency Management Committee (SEMC), on behalf of the NSW Government, commenced the NSW Emergency Management and Disaster Resilience Review (EMDRR). The review provides for a 10-year reform plan to build greater disaster resilience across NSW.

The *NSW Critical Infrastructure Resilience Strategy* is a key piece of work within the review and has been developed in conjunction the *NSW Emergency Risk Management Framework* and the *NSW 2017 State Level Emergency Risk Assessment*.

Covering emergency management areas such as community and business sector engagement, capability development, governance and lessons management, the review aims to create a safer, more secure and more disaster-resilient NSW.

Emergency Risk Management
Framework
July 2017
2017 State Level
Emergency Risk Assessment
Executive Summary
July 2017
NSW Critical Infrastructure
Resilience Strategy
Discussion Paper
September 2017
NSW Critical Infrastructure
Resilience Strategy
Partner, Prepare, Provide
NSW Department of Justice | Office of Emergency Management
NSW Critical Infrastructure
Resilience Strategy
User Resources
NSW Department of Justice | Office of Emergency Management

Critical Infrastructure Resilience Strategy suite

Executive Summary

The NSW Critical Infrastructure Resilience Strategy encourages leaders in business and government to support the NSW community by improving critical infrastructure resilience (CIR) across NSW.

NSW benefits from critical infrastructure (CI) that provides secure and reliable essential services, such as food, water, energy, transport, telecommunications and health care. Without these services, our social cohesion, economic prosperity and public safety are detrimentally affected.[1]

The CI of NSW is exposed to an increasing number of threats, hazards, shocks and stresses.[2,3] Disruptions to critical infrastructure can result in loss of life, negative economic impact and harm to communities, including psychological distress.[4] More frequent natural disasters of greater magnitude[5], and a heightened risk profile in relation to criminal threats including cyberattack[6,7], mean NSW's infrastructure and organisations must be more resilient than ever.

Long-term stresses such as increased population density, ageing infrastructure, and climate change add to the challenge of improving infrastructure resilience.[8,9]

Increased interdependencies between infrastructures can amplify consequences. Events such as Ex-Tropical Cyclone Debbie, and the 2016 and 2015 East Coast Lows caused community disruption via infrastructure service outages.[10]

Almost all infrastructure is a multi-decade investment and most infrastructure will be exposed to many hazards during its life.[11] On average, reconstruction costs due to natural disasters cost NSW $3.6bn per year with a predicted rise to $10.6bn per year by the year 2050 if we do not build resilience.[12]

This strategy promotes NSW critical infrastructure that can:

- withstand shock events to continue operating; or
- be returned to service as soon as possible after any disruption; and
- responds to long-term stresses.

A focus on physical infrastructure alone will not achieve this. This strategy has three outcomes:

- Improved **infrastructure resilience**;
- Improved **organisational resilience**; and
- Improved **community resilience**.

To achieve these outcomes, priority is given to:

- **Partnering** for shared responsibility around critical infrastructure resilience;
- **Preparing** for all hazards, not just the ones we can foresee; and
- **Providing** critical infrastructure services with minimal disruption.

Australia will spend over $1 trillion on infrastructure before 2050,[13] with New South Wales receiving a large portion of this spend. If integrated early in design, spending just an additional 1% of new infrastructure project budget can provide effective mitigation to natural hazards and climate change.[14] This contributes to savings across all phases of the asset management lifecycle, especially after a disaster, when less time and money is spent on recovery and reconstruction.

Embedding resilience in NSW infrastructure creates a "double dividend" of avoided costs from disasters, but also improvements to economic growth and social wellbeing that arise even in the absence of a disaster.[12]

Primary responsibility for Critical Infrastructure service provision sits with infrastructure owners and operators. The NSW government is committed to a collaborative and supportive partnership with infrastructure providers. This ensures that the people of NSW gain maximum service from critical infrastructure at all times.

Our more complex and interconnected infrastructure requires better plans. This strategy provides a state-wide platform to address infrastructure complexity and enhance state-wide critical infrastructure resilience.

Strategy User Resources, available through the NSW Office of Emergency Management (OEM) website, support all partners in infrastructure planning and provision in achieving the outcomes and pursuing the priorities of this strategy.

Together we can build a safer, more secure and more resilient NSW.

Strategy Benefits

Critical Infrastructure Providers (Regardless of ownership)	• Reduced business disruption • Enhanced reputations and business confidence • Reduced total cost of asset ownership and increased return on investment • Better understanding of infrastructure interconnectedness, allowing vulnerabilities to be addressed across multiple CI provider organisations • Stronger cultures to meet business challenges (not just emergency events)
For Communities	• Reduced service disruption to the people and businesses of NSW • More effective emergency management arrangements • More resilient communities, reducing the social costs of disasters
For Government	• Enhanced capability and co-ordination of response and recovery agencies • Reduced response, reconstruction, and recovery costs arising from emergency events
For all of us	• Stronger partnerships between business, government and the community • Enhanced resilience against hazards and threats • Insurance premiums that incorporate the benefits of resilience-building activity • Improved adaptation to long-term stresses such as climate change and population growth

Introduction: Critical Infrastructure Resilience

Key Terminology

Critical infrastructure (CI) is the assets, systems and networks required to maintain the security, health and safety, and social and economic prosperity of NSW. These are underpinned by the organisations and people that support them.

Infrastructure Providers include any organisation that provides NSW critical infrastructure, including privately owned organisations, local government, state government, and government-owned corporations.

Critical infrastructure Protection (CIP) focuses on mitigation against the specific threat of terrorism for CI determined to be critical to the State of NSW. CIP minimises vulnerability to criminal or malicious threats via physical, procedural, person-based, and electronic defences.[15]

In NSW the protection of CI from terrorism is managed under separate and existing arrangements. The NSW Police Force is the combat agency for terrorism.[16] The Critical Infrastructure Protection Program and Critical Infrastructure Resilience Strategy are complementary to each other.

Critical infrastructure Resilience (CIR) is the capacity of CI to withstand disruption, operate effectively in crisis, and deal with and adapt to shocks and stresses. It includes the flexibility to adapt to present and future conditions. At the national level, CIR is the term used to describe an 'all hazards' approach to CI activities across the spectrum of prevention, preparedness, response and recovery.[15]

In NSW, while infrastructure providers retain responsibility for CIR, it is delivered as a partnership between infrastructure owners, infrastructure operators, the NSW community, and local, state and federal government.

Within this strategy, CIR outcomes are divided into three categories, or types of resilience:

Infrastructure Resilience (IR) is the resilience planned for, designed, and built into assets, networks and systems.

Organisational resilience (OR) is the resilience of the organisations, personnel and processes supporting infrastructure to supply a service.

Community resilience (CR) focuses on the role the community plays in building and maintaining its own resilience while contributing to critical infrastructure resilience.

Improving Critical Infrastructure Resilience

The NSW CIR strategy is designed to have a positive impact on continued service and amenity to the people of NSW.

The strategy outcomes are grouped into three categories:

- improved **infrastructure resilience**;
- improved **organisational resilience**; and
- improved **community resilience**.

Within the strategy, infrastructure resilience (the resilience of assets, networks and systems) and organisational resilience (the resilience of organisations and processes), support community resilience (the ability of the NSW community to withstand emergencies and adapt to a new normal after major disruption). This relationship is not simple as the outcomes support and inform each other to provide a more resilient whole: improved critical infrastructure resilience.

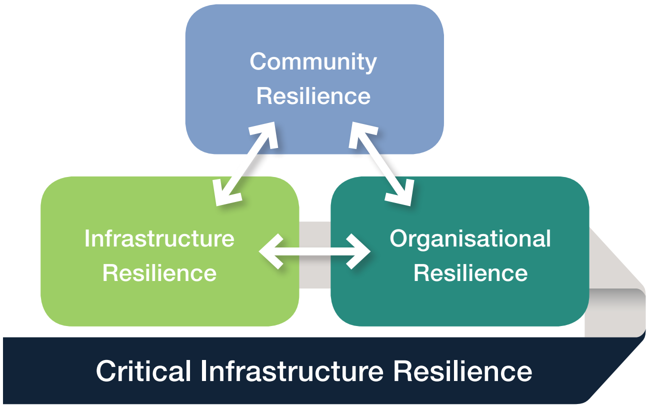

Community Resilience
Infrastructure Resilience
Organisational Resilience
Critical Infrastructure Resilience

Figure 4: CIR is improved through Infrastructure, Organisational and Community Resilience

Critical infrastructure resilience improvements help reduce other risks (e.g. resilient transport infrastructure facilitates evacuation in times of emergency).

Strategy outcomes are only listed briefly but are supplemented via user resources available at the NSW Office of Emergency Management website.

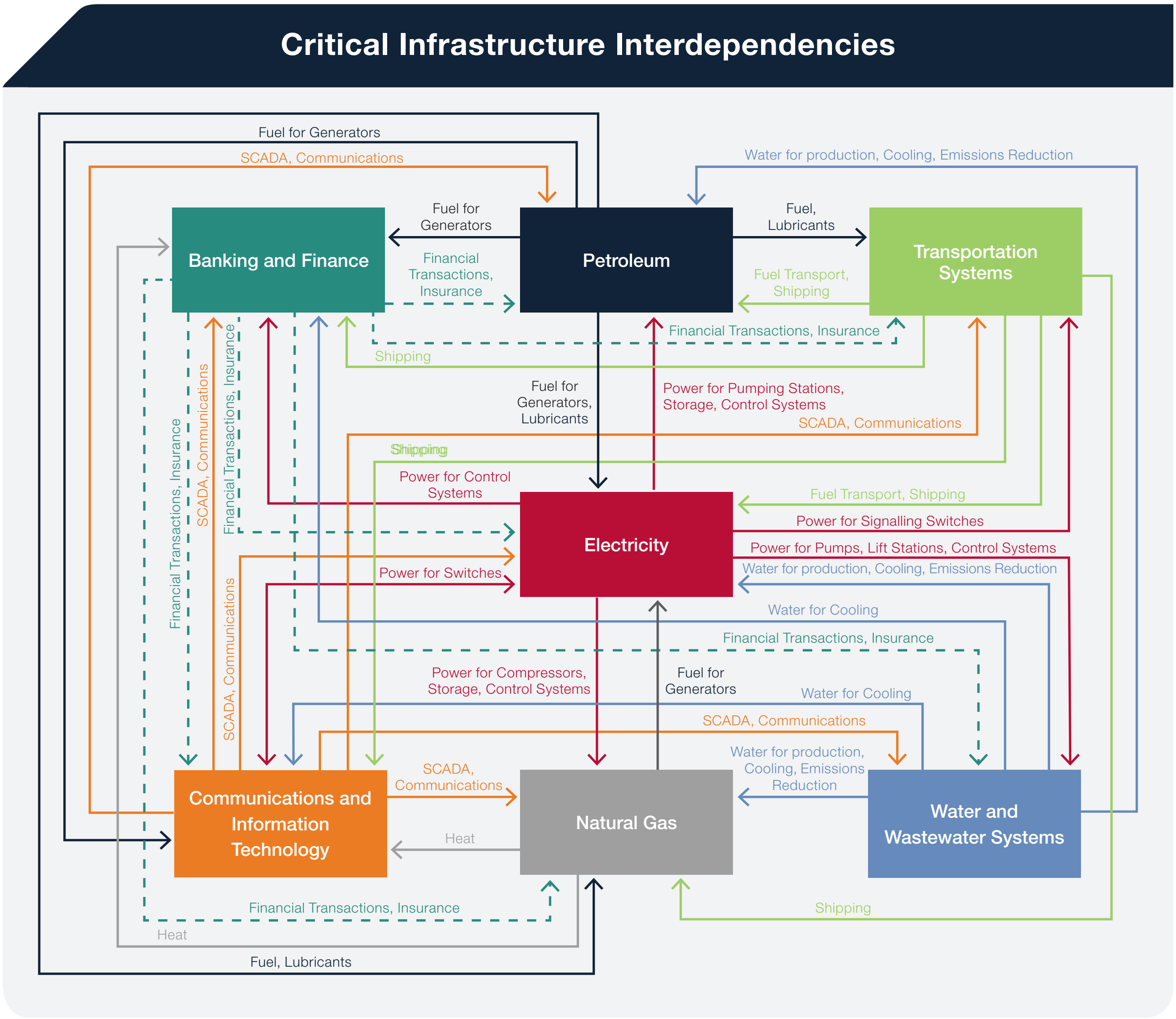
Building on Good Foundations

Wherever possible these outcomes utilise existing structures, organisations and communities at local, regional, State and Federal levels to improve CIR. Positive resilience practices are already in place in some areas but may need strengthening in others. Importantly, good practice should be embedded across NSW infrastructure to be considered business as usual.

Infrastructure Interdependency and Interconnectedness

The infrastructure that underpins everyday life in NSW is complex. Interdependency mapping highlights the need to promote resilience across the entire supply chain that delivers NSW CI. Interdependency becomes interconnectedness, and therefore a strength, when the NSW community of infrastructure providers work together to promote CIR right across NSW.

A sample interdependency model based on electricity supply illustrates the complexities in delivering essential services:



Critical Infrastructure Interdependencies

Banking and Finance
Petroleum
Transportation Systems
Electricity
Communications and Information Technology
Natural Gas
Water and Wastewater Systems
Fuel for Generators
SCADA, Communications
Water for production, Cooling, Emissions Reduction
Fuel for Generators
Fuel, Lubricants
Financial Transactions, Insurance
Fuel Transport, Shipping
Financial Transactions, Insurance
Shipping
Fuel for Generators, Lubricants
Power for Pumping Stations, Storage, Control Systems
SCADA, Communications
Shipping
Power for Control Systems
Fuel Transport, Shipping
Power for Signalling Switches
Power for Pumps, Lift Stations, Control Systems
Water for production, Cooling, Emissions Reduction
Power for Switches
Water for Cooling
Financial Transactions, Insurance
Financial Transactions, Insurance
SCADA, Communications
Financial Transactions, Insurance
SCADA, Communications
Power for Compressors, Storage, Control Systems
Fuel for Generators
Water for Cooling
SCADA, Communications
SCADA, Communications
Water for production, Cooling, Emissions Reduction
Heat
Financial Transactions, Insurance
Shipping
Heat
Fuel, Lubricants

Figure 1: Example of infrastructure system interdependencies[17]

All CI is dependent to some extent on other infrastructure to operate. The services supplied from energy, water, transport, and telecommunications underpin almost all other critical infrastructure.[15] Interdependencies can look like deficiencies in system design but during normal operation they provide efficiency and enhanced operational capability.

An integrated approach to resilience enhancement not only reflects a requirement to work together to enhance NSW CIR, it reflects the physical reality of heavily interconnected infrastructure.

Prioritising Focus: Infrastructure Criticality

Infrastructure criticality assessment models provide a good foundation for focusing resilience improvements and a common terminology for collaboration on CIR.

By using the existing long-standing system for defining the criticality of infrastructure in relation to counter-terrorism,[15] NSW is extending this use for Critical Infrastructure Protection to the all-hazards approach of Critical Infrastructure Resilience.

The system grades infrastructure on the consequence of failure, rather than the likelihood failure will occur. It also considers the likely assistance required to restore infrastructure service.

Contextual Criticality

Previously this system has been used from a state or federal perspective, which is useful for establishing reporting requirements on different classes of infrastructure.

Definitions of infrastructure criticality do however rely on perspective and purpose. What is vital for a region, may not be vital for a town. What is significant for a CI provider's own organisation, may not be as significant for the State. What is critical during one part of the year, may be less critical at other times. This recognises the size and diversity of NSW, the different expectations the community has on CI providers, and that different jurisdictions and organisations have different resources available to them in an emergency.

Within NSW, organisations are encouraged to adopt the terminology used in this model but scale the terms to assess criticality from their perspective (e.g. in business continuity planning). Simple examples are highlighted in Figure 3 below.

State	Organisation	(LG) Local Government
Vital		
State-level impact, alternative unavailable within NSW, long-term impact to NSW	Organisation-wide impact, alternative unavailable within organisation, long-term impact to organisation function	LG-wide impact, alternative unavailable within LG, long-term LG impact
Major		
State or Regional impact, major effort or assistance required to restore, medium-term impact to NSW	Impact across most of the business, major effort or assistance required to restore, medium-term impact to organisation function	Affects multiple functions of local government, major effort or assistance required to restore, medium-term impact to LG services
Significant		
Local or Regional impact, additional assistance required from within NSW, short-term impact to NSW	Impact to one or more sections of the business, other business sections provide assistance, short-term impact to organisation function	Affects one or more significant functions of LG, assistance from other parts of the LG to restore, short term impact to LG
Low		
Local impact, additional assistance may be required from within NSW, minimal impact to NSW	Impact to one part of the business, assistance from other parts of the business may be required, minimal impact to whole of business function	Impact to one function of LG, assistance from other parts of the LG may be required, minimal impact to LG function

Figure 3: Applying contextual criticality to different perspectives

Strategy User Resources, available through the NSW Office of Emergency Management website, provide further support on interconnectedness and criticality for all partners in infrastructure planning and provision.

Outcome 1: Improved Infrastructure Resilience

Infrastructure resilience is focused on the resilience planned for, designed, and built into assets, networks and systems.

The goal of improved infrastructure resilience is safer and more reliable physical infrastructure that provides service under all conditions, especially emergencies. We must strive to ensure that the CI NSW relies on every day suffers minimal disruption and is designed to be restored to operation as soon as possible after any service interruption.

Infrastructure resilience can be 'hard' or 'engineered' resilience that allows assets to withstand threats or hazards, or it can be the supply of 'soft' systems that allow for better infrastructure planning, such as land use policy and natural hazard risk data.

The Elements of Infrastructure Resilience

The four elements of infrastructure resilience are illustrated in Figure 5.[18] Improving any element of infrastructure resilience improves overall infrastructure resilience. Considering all elements when planning and designing infrastructure, markedly improves overall infrastructure resilience.

Infrastructure Resilience

Resistance	Reliability	Redundancy	Enhancing Response and Recovery
Resistance is concerned with direct physical protection. It is CI's ability to withstand shocks to continue operation (e.g. storm surge barriers built to withstand severe storms)	**Reliability** is the capability of infrastructure to maintain operation in a variety of conditions (e.g. electricity networks designed to operate in extreme heat or extreme cold)	**Redundancy** is the adaptability of an asset or network to cope with loss of individual components (e.g. a hospital with two physically separate water supplies)	**Enhancing Response and Recovery** is infrastructure resilience designed to enhance a provider's ability to recover from disruptions. (e.g. modular infrastructure for single part replacement

Figure 5: Elements of infrastructure resilience[18]

Improving Infrastructure Resilience

The graphic below identifies ways to improve infrastructure resilience. These are expanded upon within strategy user resources, available via the NSW Office of Emergency Management website.

Improving Infrastructure Resilience

Infrastructure Planning	• Integrated planning and investment • Good data enabling good decision making • Locating infrastructure in less risk-prone locations • Risk avoidance in the planning stage • Hazard mitigation
Infrastructure Design	• Resilience by design • Security by design
Infrastructure Operations and Maintenance	• Maintenance resilience – Maintenance planning – Remote sensors • Operations resilience – Faster service restoration • Reconstruction resilience – Infrastructure betterment in restoration or reconstruction

Outcome 2: Improved Organisational Resilience

Organisational Resilience refers to the resilience of the organisations, personnel and processes supporting the infrastructure to supply the service.[19]

The people and organisations that support infrastructure have as much impact on CI resilience as the assets, systems and networks themselves. Without holistic resilience across the people, systems and physical elements, the resilience of NSW CI will not improve. The NSW Critical Infrastructure Resilience Strategy encourages organisational resilience for all CI providers so they can improve together and provide a reliable and safe service to NSW.

Organisational Resilience is not just for infrastructure providers, it is also for community and business users of critical infrastructure – to ensure they have planned for what to do when interruptions to infrastructure service provision affect their organisation.

The benefits to business of enhanced Organisational Resilience are not reserved for emergencies. Enhanced Organisational Resilience improves organisational culture and ability to solve business problems.[19]

Improving Organisational Resilience

The graphic below identifies ways to improve Organisational Resilience. These are expanded upon within strategy user resources, available via the NSW Office of Emergency Management website.

Improving Organisational Resilience

Emergency Preparedness	• Exercises • Recommendation Implementation • Training
Strong Relationships	• Closer integration of NSW Emergency Management Arrangements with infrastructure providers • NSW and Federal Critical Infrastructure Networks – Sector Networks (explored further in Priority 1: Partner) – Cross-sector Networks (geographical)
Effective Risk Management	• Standards-based risk management • Tools for risk management
Improved Planning	• Emergency • Security • Business Continuity
Response and Recovery	• Improved co-ordination of response and recovery through partnerships • Formalised mutual aid agreements (within and across borders) • Alternative methods of supply or service provision • Critical spares • Pre-staging supplies and personnel

Outcome 3: Improved Community Resilience

Community Resilience focuses on the role the community plays in building and maintaining its own resilience while contributing to Critical Infrastructure Resilience. Building resilience within the community requires an integrated approach involving both government and business.

In an emergency, community response can be critical to minimising the consequences and reducing recovery effort. For example, during heatwaves when the electricity network is near capacity, community load reduction can assist the electricity network to continue to function.

Rather than just focusing on the counts of customers with a disrupted or failed service, organisations can view the community as active partners in critical infrastructure resilience, and a valuable resource before, during, and after an emergency.

A resilient community is prepared, dynamic, flexible and quick to respond. Resilient communities can mitigate against disruptive events.[20] The greater the disaster, the less likely that CI providers and government are able to provide an effective response without community assistance. The impacted community is usually located in the area and has some understanding of where outages are and the potential dangers from damaged infrastructure. The community often act as first responder, especially when individual lives are at risk (e.g. downed electricity wires). "In the case of almost any disaster, the fastest response will be from your neighbour."[21]

The community resilience component of Critical Infrastructure Resilience will be enhanced when CI providers and government prepare and support communities with consistent and reliable information, but also engage them as partners in service provision.

Improving Community Resilience

The graphic below identifies ways to improve community resilience. These are expanded upon within strategy user resources, available via the NSW Office of Emergency Management website.

Improving Community Resilience	
Community Information	• Community warnings • Community information - before, during and after service outages and emergencies
Reducing Service Disruptions	• Infrastructure investment based on community needs • Resiliency investment based on community needs
Managing Service Disruptions	• Increasing community preparedness for lack of service – Get Ready NSW[2] • Supporting vulnerable customers and communities – More rapid service restoration – Advice to vulnerable customers – Allocation of emergency resources to vulnerable customers
Community Partnership	• Community engagement • Community partnerships • Community input into emergency risk planning and management • Mutual assistance (e.g. Public reporting suspicious behaviour around CI) • Crowdsourcing emergency information and intelligence (e.g. Social media)

Priority 1: Partner

We must **Partner** in shared responsibility for critical infrastructure resilience.

Partner: Shared Responsibility

Resilience improvement is best effected when CI providers partner with all levels of government and the community in shared responsibility.[22] This recognises the diverse perspectives and shared skills that all parties bring to increasing resilience. It also recognises that consequences of infrastructure failure affect many parts of the NSW community, not just the infrastructure providers themselves.

Relationships in Shared Responsibility

This strategy promotes a non-regulatory partnership approach to critical infrastructure resilience. It encourages closer working relationships between government and infrastructure providers, in line with the Australian Government's *Critical Infrastructure Resilience Strategy*.[1] Where CI Providers already work with existing regulatory agencies, government departments, or emergency management agencies, these relationships remain key to enhancing CIR.

Under this approach, CI providers retain ultimate responsibility for the safety and security of their assets and of service provision to their customers and the NSW community. This approach recognises the fact that CI providers are best placed to effectively manage risks to their infrastructure.[1]

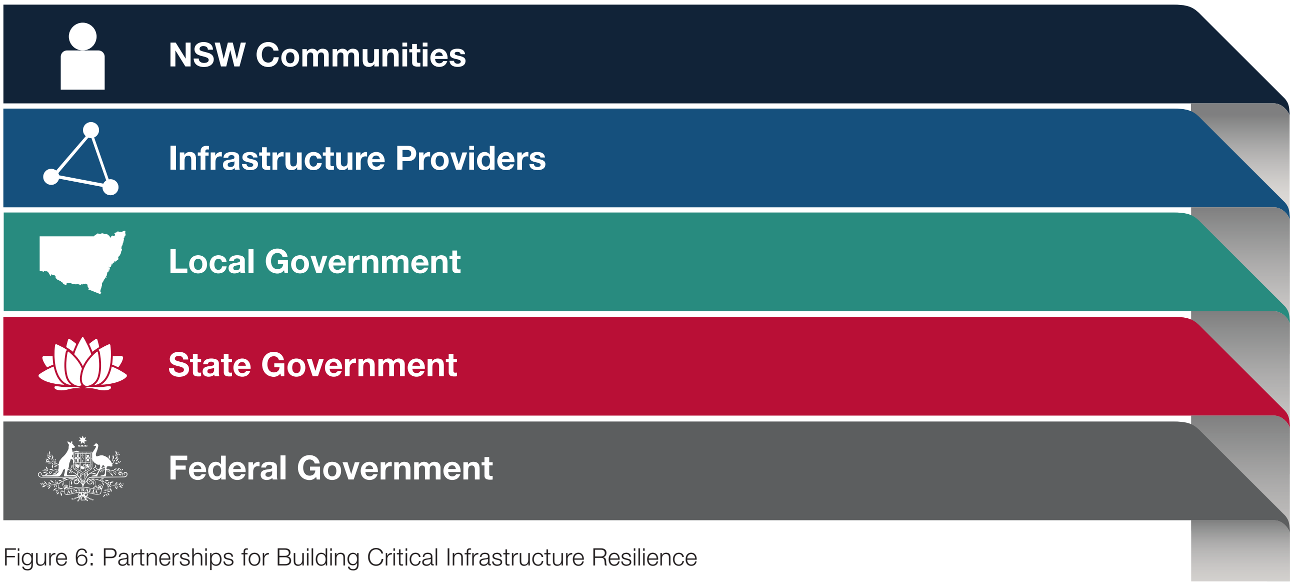


Figure 6: Partnerships for Building Critical Infrastructure Resilience

Further information surrounding the roles played by each of these partners in CIR can be found in the Appendix: Roles within NSW CIR Arrangements.

Key Initiative: Sector Networks

The NSW Government promotes closer relationships with, and between, infrastructure providers and emergency management organisations to foster enhanced CIR.

In line with the approach of building on good foundations, the NSW Government encourages the use of the existing Trusted Information Sharing Network (TISN) co-ordinated via the Commonwealth Home Affairs Department. TISN is a platform for business-government information sharing and resilience-building initiatives and broadens the pool of sector-specific experience for NSW CI professionals to the national level.[23] Where TISN sector groups do not exist (for NSW government and Education), separate NSW sectoral groups are facilitated via the NSW State Emergency Management Committee's Critical Infrastructure Review Working Group.

The introduction of an Education Sector group within NSW reflects the importance of education in the functioning of resilient communities, in line with the United Nation's Sendai Framework for Disaster Risk Reduction.[24] Disaster recovery is accelerated by a properly functioning education system.[25] This also acknowledges the NSW Department of Education's commitment to integrate their infrastructure more closely with communities[26] and a general commitment across all schools to work closely with communities.

Cross-sectoral collaboration is facilitated geographically at the state, regional and local level. CI providers are invited to attend Local and Regional Emergency Management Committees as part of this strategy. The relationships strengthened via cross-sectoral geographic meetings are expected to increase the capability of local emergency management to respond to and recover quickly from local emergencies.[27]

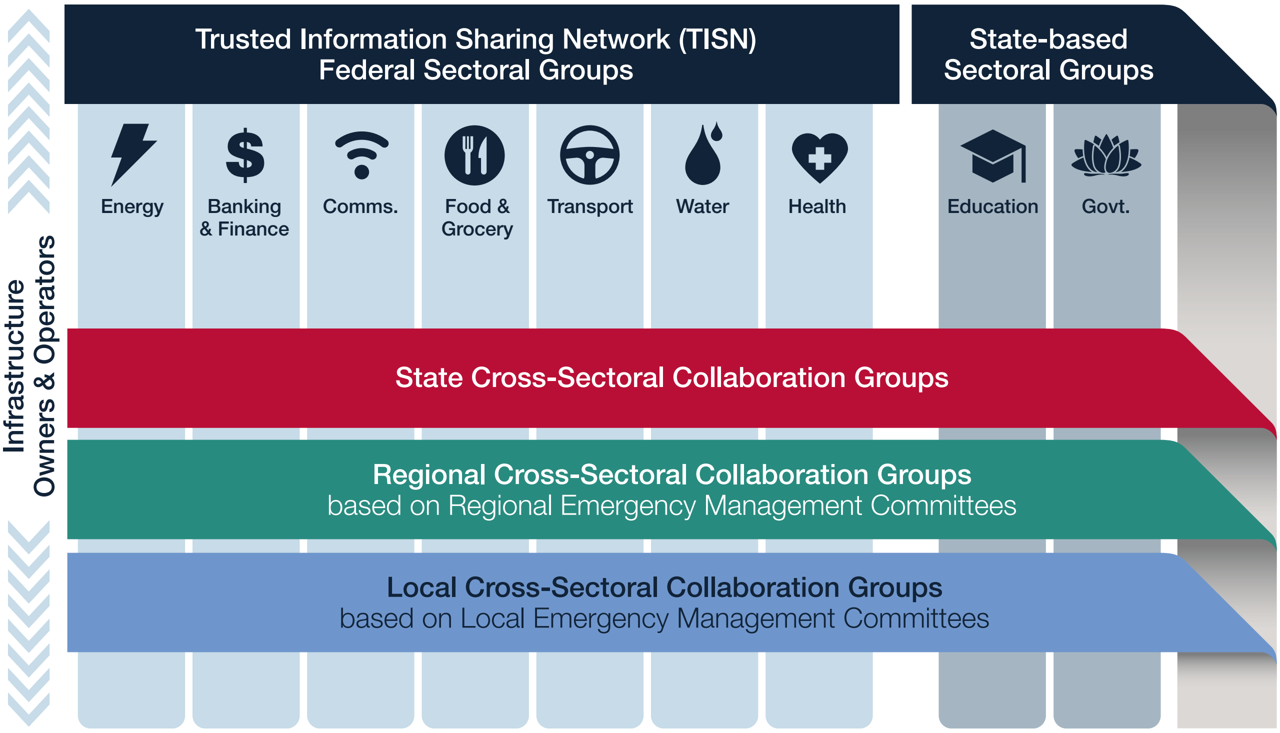

Trusted Information Sharing Network (TISN)
Federal Sectoral Groups
State-based
Sectoral Groups
Energy
Banking & Finance
Comms.
Food & Grocery
Transport
Water
Health
Education
Govt.
Infrastructure Owners & Operators
State Cross-Sectoral Collaboration Groups
Regional Cross-Sectoral Collaboration Groups
based on Regional Emergency Management Committees
Local Cross-Sectoral Collaboration Groups
based on Local Emergency Management Committees

Figure 7: Sectoral and Cross-Sectoral Groups

Further information surrounding the roles played by each of these partners in CIR can be found in the Appendix: Roles within NSW CIR Arrangements.

Priority 2: Prepare

We must **Prepare** for all threats and all hazards, not just the ones we can foresee.

Prepare: All Threats/All Hazards/All Shocks/All Stresses

An all-threats and all-hazards approach to Critical Infrastructure Resilience (CIR) is particularly effective for unexpected shock events, as well as anticipated shocks and long-term stresses.

Focusing on building resilience requires careful consideration of the risks that infrastructure is exposed to and developing ways to mitigate against these risks. By adopting the all hazards approach, specific risk treatment measures can be adjusted to address multiple risks and also build resilience against unanticipated risks. This is also true where interconnections to other infrastructure networks may have been underappreciated in the past. The all threats, all hazards approach allows CI Providers to focus on the consequences of infrastructure disruption (e.g. loss of amenity to people, businesses and community), rather than the cause of the disruption. This will produce cost-effective solutions that are more likely to address multiple threats or hazards.

Threats

Threats are criminal or malicious acts or intent to disrupt the operation of CI. The motivations for criminal or malicious acts and threats are sometimes different, but the effects on CI can be very similar. Threats can occur in a variety of ways including terrorism, sabotage, espionage and cyberattack.

Responsibility for responding to criminal or malicious acts is maintained by the appropriate state or federal agency. Critical Infrastructure owners have a responsibility to maintain appropriate physical and cybersecurity protections.

There is an increasing focus on the threat of cyberattack. The NSW and Commonwealth governments take a shared approach to providing information, advice and support to infrastructure owners and operators on cybersecurity.[28,29]
The case study, Improving NSW Resilience to the Continued Threat of Cyberattack, highlights the potential serious consequences of cyberattack for CI owners and operators.

Hazards

Hazards include extreme weather events, equipment failure and accidents.

New South Wales is frequently exposed to these events, such as storms and bush fires, but also the less common biosecurity and pandemic outbreaks. These events have the potential to severely disrupt supply chains that CI relies on.

The *NSW 2017 State Level Emergency Risk Assessment* highlights the key natural hazards NSW is likely to face.[2] It assists CIR by providing a high-level risk assessment of significant natural hazard events at a state level.

Technical hazards include aged assets, mechanical or technological failure, and accidents. These events sometimes have the potential to create cascading failures that have wide-ranging consequences due to infrastructure interdependencies. Increased CIR is an effective mitigation against technical hazards.

Shocks

Shocks are sudden, sharp events that have the potential to disrupt the services supplied via infrastructure. Shocks can be from threats or hazards and are often sudden onset.

Stresses

Long-term stresses such as ageing infrastructure, population density, or the increasing interdependencies between Critical Infrastructures can amplify shock events.[3] Climate change is a stress that exacerbates the impacts of threats and hazards.[22]

The state government provides tools such as the *State-Level Emergency Risk Assessment*,[2] and AdaptNSW[30] to assist CI providers to understand the long-term impacts around natural hazards and climate change. As recommended within the *NSW State Infrastructure Strategy*, integrating CIR in all phases of the asset management cycle, particularly in planning and design, assists with the mitigation of long-term stresses.

Key Initiative: Infrastructure Resilience Training and Exercises

Australian CEOs see scenarios, exercises and training as key tools for building trust and embedding a resilience culture in their organisations.[31]

This strategy builds on the existing provision of emergency management training by the NSW government, initially with CIR-specific training aimed at Local Emergency Management Officers, and subsequently provided for all stakeholders in CIR over the course of the strategy. Registered organisations will be able to use this training within their own CIR programs to enhance the knowledge and understanding of their staff in improving CIR across NSW.

As part of this strategy, the NSW State Exercise Program has highlighted CI-focused exercises as a priority. This will facilitate the inclusion of CI exercises at the state, regional and local level. The closer integration of CI providers into exercise design, conduct, and evaluation, will allow all NSW organisations to exercise around the impact of threats, hazards, and stresses to critical infrastructure.

A strong CIR training and exercise program will not only prepare CI providers and emergency services for threats, hazards and stresses, it will also help grow a culture of resilience in the participating organisations themselves, allowing them to better adapt not only to emergency situations, but also to business challenges and unusual problems.

Source: Sharon Quandt 2017

Priority 3: Provide

We must **Provide** critical infrastructure services with minimal interruptions.

Provide: Services with Minimal Disruption

The Cost of Critical Infrastructure Service Interruption

Customers of CI services are sometimes unaware of the complexities of the infrastructure itself but are usually very aware of the reduction in public and business amenity that CI service outages cause.

Along with the risks to health and safety, there are significant economic impacts of service interruption. Cost estimates can be difficult to quantify, but losing just one essential service such as electricity, in the Sydney CBD for four hours could cost $136 million for every 200 MW of unserved load.[32] The cost of electricity outages over a long period of time or a large area of NSW is likely to be measured in the hundreds of millions of dollars.

Of course, no CI service is immune to disruptions, but improved resilience allows for increased resistance to shocks and more rapid recovery from outages.

Planning and Designing Resilient Services

The best time to embed resilience in infrastructure services is in the early stages, during planning and design. The World Bank estimates that, if integrated early in the design phase, spending just an additional 1% of new infrastructure project budget can provide effective mitigation to natural hazards and climate change.[33] This contributes to savings across the entire lifecycle of infrastructure and is especially true after a disaster, when less time and money is spent on re-establishing services.

The community benefits of embedding resilience thinking into the planning, design and operation of services from infrastructure create a double dividend of avoided costs from disasters, but also co-benefits that arise even in the absence of a disaster.[12]

Australia is projected to spend $1.1 trillion on infrastructure before 2050.[13] New South Wales infrastructure will comprise a large portion of this spend. More important than the cost of the infrastructure is the service and increased amenity that the infrastructure will provide.

Embedding resilience thinking in service planning and design will ensure the infrastructure built today will provide reliable services to NSW business and communities for a long time to come.

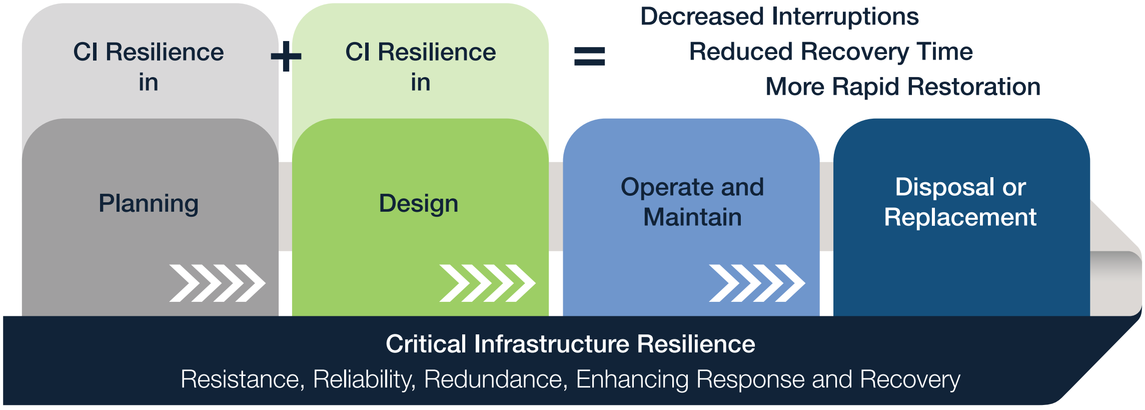


Figure 8: Embedding Resilience in the Planning and Design of Services pays back during Operation and Maintenance of Services

Key Initiative: User Resources

The NSW Office of Emergency Management is co-ordinating the provision of user resources under this strategy to provide best-practice advice from NSW and around the world on how to implement CIR.

This strategy provides the 'why' of CIR and the user guides provide the 'how' of CIR.

The resources focus on the resilience measures identified in each of the sections on infrastructure resilience, organisational resilience and community resilience, and include:

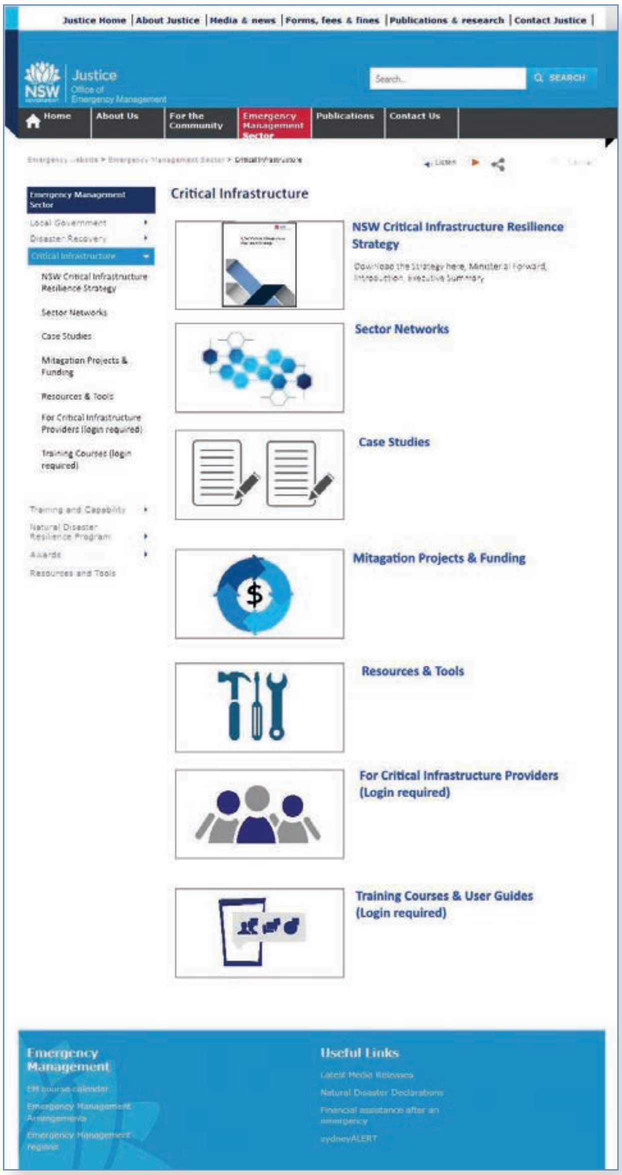
- Case studies including best practice examples
- Support tools for increased emergency preparedness through training and exercises
- Sources of resilience improvement project funding
- Advice on cost / benefit analysis of mitigation investment
- Integrating good resilience practice into infrastructure planning, design, operations and maintenance
- Risk management tools and processes
- Emergency, security and business continuity planning
- Enhancing response and recovery from disruption
- Enhancing community information and partnerships

Some resources will focus on specific infrastructure sectors. Others will focus on specific topics such as cost/benefit analysis or infrastructure resilience project funding.

CIR strategy user resources are expected to benefit:

- Infrastructure providers
- Emergency, security and resilience managers
- Risk and business continuity managers
- Land-use planners at local and state level
- Infrastructure engineers and designers
- Asset managers
- Local, regional and state emergency management committees
- Insurance providers and infrastructure funding bodies
- Researchers

A local government user resource, designed to support the strategy throughout NSW, is available via the NSW Office of Emergency Management website. Many tools in this user resource will be useful to all partners in the provision of CI. Further user resources will be released and updated across the life of this strategy and made available via the NSW Office of Emergency Management website. www.emergency.nsw.gov.au/CriticalInfrastructure


Justice Home | About Justice | Media & news | Forms, fees & fines | Publications & research | Contact Justice |
NSW
Justice
Office of Emergency Management
Search...
SEARCH
Home
About Us
For the Community
Emergency Management Sector
Publications
Contact Us
Emergency Website > Emergency Management Sector > Critical Infrastructure
Listen
Emergency Management Sector
Local Government
Disaster Recovery
Critical Infrastructure
NSW Critical Infrastructure Resilience Strategy
Sector Networks
Case Studies
Mitagation Projects & Funding
Resources & Tools
For Critical Infrastructure Providers (login required)
Training Courses (login required)
Training and Capability
Natural Disaster Resilience Program
Awards
Resources and Tools
Emergency Management
EM course calendar
Emergency Management Arrangements
Emergency Management regions
Useful Links
Latest Media Releases
Natural Disaster Declarations
Financial assistance after an emergency
sydneyALERT

Critical Infrastructure

NSW Critical Infrastructure Resilience Strategy

Download the strategy here, Ministerial Forward, Introduction, Executive Summary

Sector Networks

Case Studies

Mitagation Projects & Funding

Resources & Tools

For Critical Infrastructure Providers (Login required)

Training Courses & User Guides (Login required)

Conclusion:
A Safer, More Secure, More Resilient NSW

By pursuing the **Infrastructure Resilience**, **Organisational Resilience**, and **Community Resilience** outcomes highlighted in this strategy, New South Wales critical infrastructure will be better prepared for emergency events.

Key initiatives already underpin the three priorities of:

- **Partnering** for shared responsibility around infrastructure resilience;
- **Preparing** for all hazards, not just the ones we can foresee; and
- **Providing** reliable essential services to the businesses and communities of NSW.

The NSW Critical Infrastructure Strategy User Resources will provide support to all partners in infrastructure planning and provision in achieving the outcomes and pursuing the priorities of this strategy.

Withstanding the shocks of threats and hazards, preparing for long-term stresses, and returning NSW infrastructure to operation as soon as possible requires a combined effort from communities, business, and all levels of government.

By Partnering, we can share the best approaches to improved resilience, by Preparing we can be ready for all hazards and all threats, and by embedding resilience in our thinking we can Provide reliable essential services to the businesses and communities of NSW.

Our more complex and interconnected infrastructure requires better planning. This strategy provides a state-wide platform to address infrastructure complexity and enhance state-wide Critical Infrastructure Resilience.

The strategy has a five-year lifespan, with a mid-term review to determine our effectiveness in pursuing the strategy outcomes and building Critical Infrastructure Resilience in NSW.

Together we can build a safer, more secure, and more resilient NSW.

Today, we are planning and building the infrastructure we will be using in 2050, in what will be a very different climate and a very different New South Wales. We must integrate resilience into today's infrastructure to provide for tomorrow's prosperity.

Troy Grant
Minister for Emergency Services

Appendix A: Roles within NSW CIR Arrangements

Roles in Shared Responsibility

The NSW government is committed to a collaborative and supportive partnership with infrastructure providers and all elements of the NSW community to enhance Critical Infrastructure Resilience (CIR).

The primary responsibility for providing Critical Infrastructure (CI) services resides with infrastructure owners and operators. CI providers are also responsible for the security of their assets and the safety of their staff. Government and the community will partner in supporting critical infrastructure for the benefit of NSW. Many entities fulfil multiple roles and responsibilities for CI (e.g. local and state government fill both government and provider roles).

Table 1: Roles within NSW Critical Infrastructure Resilience

NSW Communities

- Individuals and communities sharing responsibility to prevent, prepare for, respond and recover from emergencies[22]
- Have an awareness of the threats and hazards that affect their locality[22]
- Be involved in emergency management arrangements, perhaps by volunteering[22]
- Build community support networks ahead of emergencies
- Individual resilience – prepare for prolonged outages without external assistance or essential services
- Respond to government advice on the use of CI (e.g. demand reduction in times of stress to electrical networks)
- Help CI providers by reporting damage to CI
- Report suspicious behaviour around infrastructure
- Use CI (e.g. transport) responsibly

Infrastructure Providers

- Provision of CI service to customers under existing legal, regulatory and business arrangements
- Meet or exceed existing legal, regulatory and business requirements
- Primary responsibility for managing hazard and threat risk to CI assets they own or manage
- Understanding the risks to infrastructure and ensuring provision of services during or soon after an emergency[22]
- Appropriate level of security for assets they own or manage
- Report incidents or suspicious activity to police
- Appropriate level of emergency / security / business continuity planning for level of risk
- Appropriate level of exercising / testing plans including inter-agency exercises
- Underpin economic and social recovery of communities
- Build community understanding and education on CIR and resilience in general

Local Government

- Meet or exceed existing legal, regulatory and business arrangements
- Build resilience (not just CIR) within the local government area. Participate in regional resilience building, including through shared arrangement with other local governments such as Joint Organisations and Regional Organisations of Councils
- Provide advice and education on hazards and threats within local government jurisdiction
- Provide land use planning and disaster mitigation functions
- Support and manage the natural environment impacting critical infrastructure
- Provide local emergency and consequence management planning via Local Emergency Management Committee
- Support LEOCON and assigned combat agency in response to local-level emergencies

State Government

- Meet or exceed existing legal, regulatory and business arrangements
- Co-ordinate resilience enhancements (not just CIR) across the state
- Provide advice on threat and hazard risk to NSW communities, businesses and infrastructure providers.[1]
- Integrating Climate Change adaptation into government assets and services
- Support SEOCON and assigned combat agency in response to state-level emergencies
- Assess risks to government services and plan to manage disaster impact
- Provide CI protection advice via NSW Police and Office for Police[1]
- Work co-operatively under counter-terrorism and security arrangements
- Provide strategic coordination of CIR across NSW via the Critical Infrastructure Review Working Group (CIRWG)
- Provide preparedness support to CI providers via training, advice and exercise management[1]
- Provide emergency response via established agencies
- Provide State Emergency Management Committee (SEMC) and state-wide emergency and consequence management plans
- Support land use planning and disaster mitigation functions
- Provide cybersecurity support, governance and coordination before, during and after incidents to government agencies through the Government Chief Information Security Officer (GCISO)

Federal Government

- Meet or exceed existing legal, regulatory and business arrangements.
- Building disaster resilience across Australia through existing services and forums (e.g. TISN)
- Warn of specific threats relating to terrorism, espionage, sabotage or coercion
- Work co-operatively under existing counter-terrorism and security arrangements
- Work co-operatively under existing espionage arrangements
- Provide advice and support on cybersecurity threats, risk and mitigation strategies
- Assist with response to cyberattacks on CI providers
- Assist with investigation of cyberattacks on CI providers

[1] For the threat of terrorism, refer to established NSW Counter Terrorism arrangements and the Critical Infrastructure Protection Program for roles and responsibilities of State Government agencies. This includes terrorism themed exercises.

Appendix B: Case Studies

Case Study 1: Integrating Infrastructure Resilience into Planning Processes: The Emilie Serisier Bridge

Flooding of a state highway bridge that crosses the Macquarie River in regional NSW has caused six major traffic disruptions since its construction in 1987, estimated to have cost about $17 million. The cost of future disruption events is estimated at $75 million, totalling about $92 million (in present value terms) over the projected life of the asset.[13]

Lifetime costs of repeated closures to the Emile Serisier bridge in Dubbo, NSW, due to floods are about $92m

When the Emile Serisier Bridge is inundated, traffic must be diverted to the LH Ford Bridge, which can withstand a one-in-50-year flood. During a 2010 flood, it took more than two hours to cross the river – a trip that typically takes 10 minutes. The increased travel time impacts other services supplied via this infrastructure, including health, emergency services, and education. There are increased costs to affected business, especially tourism, and additional social costs to the community. As the river crossing is a significant trade route, this had wider ranging impacts to regional and interstate commerce.[13]

The NSW Government is planning for a new bridge over the Macquarie River in Dubbo and has identified a preferred route.[34]

Should the new bridge cost less than $92 million this new investment will provide a net benefit to NSW critical infrastructure resilience.

Whatever the cost of the new bridge, it is likely to cost more than it would have to integrate flood resilience into the initial bridge-building project in 1987. Flood risk and infrastructure resilience is better understood today than it was in 1987, and part of the work of the NSW CIRS is to highlight the benefits of integrating resilience early to avoid reconstruction and replacement costs, and to foster the ability to gather improved data and partner in planning for resilient infrastructure.

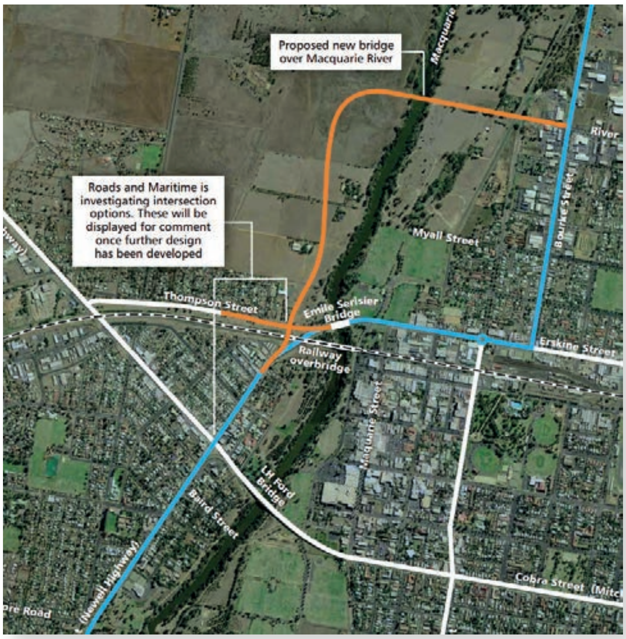


Figure 9: Preferred Route Option: New Dubbo Bridge[34]

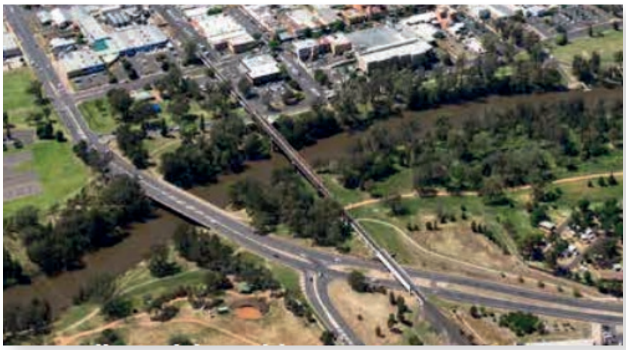


Figure 10: Dubbo, looking east over Emile Serisier Bridge[34]

Original source: http://www.rms.nsw.gov.au/documents/projects/western-nsw/dubbo-bridge/new-dubbo-bridge-map.pdf

With thanks to RMS and the Australian Business Round Table for Disaster Resilience & Safer Communities

Case Study 2: Origin Energy: Business Continuity Systems for Increased Organisational Resilience

Maintaining the continuity of critical business processes is key to Origin's role of delivering reliable energy to customers and the communities they live in.

To provide clear visibility over the entire business, Origin developed an approach to enhance and futureproof the business continuity process via an automated cloud-based system.

The approach follows the standard steps of business continuity management:

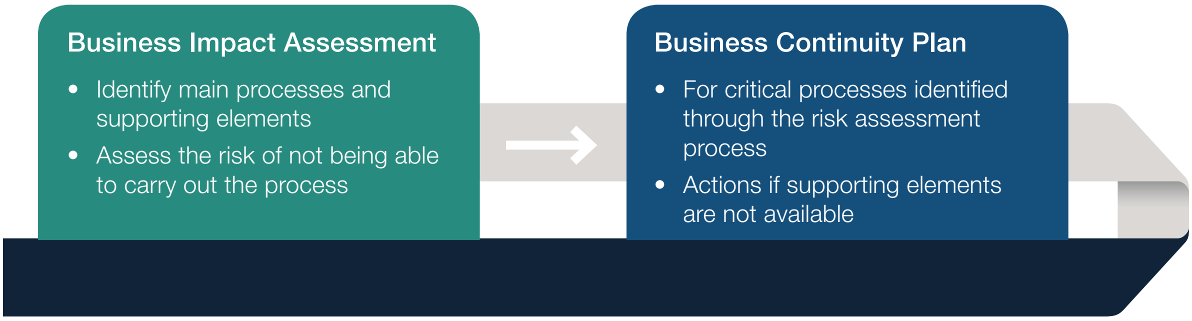

Business Impact Assessment
Identify main processes and supporting elements
Assess the risk of not being able to carry out the process
Business Continuity Plan
For critical processes identified through the risk assessment process
Actions if supporting elements are not available

Figure 11: Overview of the Business Continuity Management Process

The establishment of the automated cloud-based system provides Origin immediate visibility of preparedness and expected capability to respond to any interruption. Integrating Origin's risk management framework meets the needs of a dynamic and growing organisation.

This approach allows better analysis and greater understanding of critical processes across Origin, including tolerable outage times and dependencies.

Centralised data provides a view of internal and external interdependencies and potential vulnerabilities. More data provides a more accurate picture of Origin's business interruption risk and an enterprise wide view of critical processes and interdependencies across many diverse teams, business divisions and regions.

Current and consistent data gives business leaders the ability to prioritise resources and target activities to reduce the potential consequence of a business interruption to their areas.

Origin is expanding the system to simplify and modernise exercise and incident management. Actual interruptions will be managed on-line using the system to access current continuity plans from any device, automate task management (e.g. recovery task allocation and completion tracking), share data in real-time, ability to coordinate multiple events from one location, and track progress of multiple teams and plans at the same time.

As implementation continues and more data captured and analysed, the team can highlight areas for improvement, help develop strategies to minimise or close any gaps, and enhance capability to prepare for and respond to business interruptions.

Figure 12: Origin business activities across the energy supply chain require resilience [35]

origin

With thanks to Origin Energy

Case Study 3: FISH and FloodSmart Parramatta: Partnerships in Infrastructure for Increased Community Resilience

The City of Parramatta is one of the most flash-flood affected cites in Australia with over 23,000 homes and businesses assessed as flood-prone. Deep and fast-flowing flood water can occur in highly-populated locations with less than 6 hours' notice. Hundreds of thousands of people and key services providers may have little time to protect themselves or essential city infrastructure and services.

From a community perspective, approximately one-third of Parramatta's population moved there after 1990, with the last major floods in 1986 and 1988. These residents have no direct experience of the potential extent and severity of flooding in their local area.

To manage these risks and improve resilience to flash flooding, the City of Parramatta partnered with the NSW State Emergency Service, Bureau of Meteorology (BOM), Sydney Water and the NSW Office of Environment and Heritage to develop a flash flood warning service - the '**Parramatta River Flood Information System Hub**' or **FISH**.

FISH pulls together real-time river and rain gauge data from sensors and joins this data with the BOM's cutting-edge rainfall forecast service. A fast flood model produces a flood forecast for emergency planners. The FISH visualises data and maps through an online portal. The data can be easily accessed via smartphone or tablet and shared, allowing for targeted, fast and informed response during a flood incident.

FISH partners include infrastructure providers such as Sydney Water and Transport for NSW to provide information and warnings so other types of infrastructure are better protected from Parramatta River flooding. FISH also partners with emergency services providers for better flood emergency response and recovery.

FloodSmart Parramatta is the community interface to the FISH. The community and business sign up for free flood warnings, based on data from the FISH. FloodSmart also improves community resilience by providing access to flood risk maps, guides for flood preparedness and real-time gauge data.

The City of Parramatta knows that they can't stop floods happening, but they can help provide the infrastructure, and work in partnerships, to ensure that everyone stays safe.

Figure 13: The Parramatta River in Flood[36]

With thanks to:

Australian Government Bureau of Meteorology

FloodSmart Parramatta

City of Parramatta

NSW Government Office of Environment & Heritage

SES NSW State Emergency Service

Sydney Water

Case Study 4: Improving NSW Resilience to the Continued Threat of Cyberattack

A large amount of Critical Infrastructure relies on technological systems for operation and remote control. Although many cyberattacks on critical infrastructure are suspected, the first publicly confirmed widespread outage caused by cyberattack case was in December 2015 in the Ukraine. Over 225,000 customers across three regional electricity distributors experienced electricity supply loss.[37]

While Australia is comparatively resilient to cyberattack[38], the threat of electronic breach and misuse of systems is an ever-evolving one, due to the development of new attack technologies and systems.[6] The Australian Cyber Security Centre provides mitigation strategies for Australian businesses that require continued effort in defending against cyberattack.[39]

The NSW Critical Infrastructure Resilience Strategy is looking to endorse the Australian Government's National Cyber Partnership to assist in the creation of strong cyber defences.[40] The threat of cyberattack is a continuing one.

Critical infrastructure providers are working hard to mitigate against this threat, and all hazards and threats, to create critical infrastructure resilience for NSW.

Appendix C: Abbreviations and Glossary

Abbreviation	Meaning
All Hazards	An approach to manage the uncertain nature of emergency risk by building resilience to all or multiple hazards
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection (protection against terrorism specifically)
CIR	Critical Infrastructure Resilience (protection against all hazards)
Dependency	When a critical infrastructure relies on another critical infrastructure, good or service for continued service provision
Disaster	When a hazard or threat intersects with a vulnerability, and the ability of local resources or business as usual to cope is overwhelmed
EMDRR	NSW Emergency Management and Disaster Resilience Review
Hazard	A hazard, usually natural, that unintentionally disrupts critical infrastructure service provision
Infrastructure Provider	An organisation responsible for providing an infrastructure service at a state, regional or local level, whether publicly or privately owned
Interdependency	When multiple critical infrastructures rely on each other for continued service provision
LEOCON	Local Emergency Operations Controller
Mitigation	Measures taken in advance to reduce the likelihood or consequence of a hazard or threat.
OEM	NSW Office of Emergency Management
Resilience (Hard)	Hard resilience is generally focussed on assets, networks or systems. Examples include levees and reinforced structures.
Resilience (Soft)	Soft resilience is generally focussed on organisations, people and behaviour. Examples include policy and process, emergency and business continuity planning and community engagement.
Sector	An industry or service group identified within the NSW CIR strategy
SEMC	State Emergency Management Committee
SEOCON	State Emergency Operations Controller
SCADA	Supervisory Control and Data Acquisition (SCADA) systems are used for remote monitoring and control in the delivery of critical services such as electricity, gas, water, waste and transportation.
SLERA	NSW State Level Emergency Risk Assessment
Threat	A hazard, usually man-made, that deliberately disrupts critical infrastructure service provision
TISN	Trusted Information Sharing Network (information sharing network co-ordinated by Commonwealth Home Affairs Department)
Vulnerability	The mechanism by which critical infrastructure can be affected by threats and hazards

Appendix D: References

[1] Commonwealth of Australia. 2015. *Critical Infrastructure Resilience Strategy: Policy Statement*.

[2] State of New South Wales through Office of Emergency Management. 2017. *NSW State Level Emergency Risk Assessment*.

[3] 100 Resilient Cities. *What is Urban Resilience?*

Available at http://www.100resilientcities.org/resources/

[4] Australian Business Roundtable for Disaster Resilience & Safer Communities. 2016. *The Economic Cost of the Social Impact of Natural Disasters*.

Available at http://australianbusinessroundtable.com.au/our-papers/social-costs-report

[5] State of New South Wales through Office of Environment and Heritage. 2016. *About Climate Change in NSW*.

Available at http://climatechange.environment.nsw.gov.au/About-climate-change-in-NSW

[6] State of New South Wales through NSW Police Force. Secure NSW: *The Current Security Environment*.

Available at https://www.secure.nsw.gov.au/the-current-security-environment/

[7] Commonwealth of Australia. 2017. *Australian Cyber Security Centre 2017 Threat Report*.

[8] Organisation for Economic Co-operation and Development 2012. *Global Modelling of Natural Hazard Risks, Enhancing existing capabilities to address new challenges*.

[9] State of New South Wales through Office of Environment and Heritage. 2016. *NSW Climate Change Policy Framework*

[10] NSW Office of Emergency Management 'Reports and Corporate Publications'

https://www.emergency.nsw.gov.au/Pages/publications/reports-and-corporate-publications.aspx

[11] Infrastructure Australia. 2016. Australian Infrastructure Plan: Priorities and Reforms for our Nation's Future.

Available at: http://infrastructureaustralia.gov.au/policy-publications/publications/files/Australian_Infrastructure_Plan.pdf

[12] Australian Business Roundtable for Disaster Resilience & Safer Communities. 2017. *Building resilience to natural disasters in our states and territories*.

Available at: http://australianbusinessroundtable.com.au/assets/documents/ABR_building-resilience-in-our-states-and-territories.pdf

[13] Australian Business Roundtable for Disaster Resilience & Safer Communities. 2016. *Building Resilient Infrastructure*.

Available at http://australianbusinessroundtable.com.au/our-papers/resilient-infrastructure-report

[14] The International Bank for Reconstruction and Development / The World Bank. 2010. *The Cost of Adapting to Climate Change for Infrastructure*.

[15] Commonwealth of Australia. 2015. *National Guidelines for Protecting Critical Infrastructure from Terrorism*.

[16] State of New South Wales through NSW Police Force. Secure NSW: *Working with NSW Businesses*.

Available at http://www.secure.nsw.gov.au/what-we-do/working-with-nsw-businesses/

[17] Verner, Duane, Frederic Petit, and Kibaek Kim. 2017. *Incorporating Prioritization in Critical Infrastructure Security and Resilience Programs*. Homeland Security Affairs 13, Article 7 (October 2017)

https://www.hsaj.org/articles/14091

[18] Adapted from: United Kingdom Cabinet Office. 2011. *Keeping the Community Running: Natural Hazards and Infrastructure*.

Available at https://www.gov.uk/government/publications/keeping-the-country-running-natural-hazards-and-infrastructure

[19] Commonwealth of Australia. 2017. *Organisational Resilience*.

Available: https://www.organisationalresilience.gov.au/Pages/default.aspx

[20] Australian Business Roundtable for Disaster Resilience and Safer Communities. 2014. *Building Our Nation's Resilience to Natural Disasters*

[21] Fugate, W. Craig. *The Public as a Resource*. 2017. Emergency Management Magazine.

Available: http://www.govtech.com/em/disaster/The-Public-as-a-Resource.html

[22] Commonwealth of Australia. 2011. *National Strategy for Disaster Resilience – Building the resilience of our nation to disasters*.

[23] Trusted Information Sharing Network for Critical Infrastructure Resilience.

Available: https://www.tisn.gov.au/Pages/default.aspx

[24] UNISDR. 2015. *Sendai Framework for Disaster Risk Reduction 2015-2030*.

[25] UNISDR. 2014. *Comprehensive School Safety*.

Available at http://education4resilience.iiep.unesco.org/en/node/552

[26] State of New South Wales through New South Wales Department of Education. *School Infrastructure NSW*.

Available at https://schoolinfrastructure.nsw.gov.au/about-us

[27] State of New South Wales through Office of Emergency Management. 2016. *State Recovery Co-ordinator Report, June 2016 East Coast Low*

[28] State of New South Wales through Office of Finance and Services. 2015. *NSW Government Digital Information Security Policy*

[29] Commonwealth of Australia. *About the Australian Cyber Security Centre*

Available: https://acsc.gov.au/about.html

[30] State of New South Wales through the Department of Environment and Heritage. *AdaptNSW*.

Available at http://climatechange.environment.nsw.gov.au/

[31] Commonwealth of Australia. 2012. *CEO Perspectives on Organisational Resilience*.

Available at https://www.organisationalresilience.gov.au/resources/Documents/ceo-perspectives-on-organisational-resilience.pdf

[32] State of New South Wales through Office of the Chief Scientist & Engineer. 2017. *Final report from the Energy Security Taskforce*.

[33] The International Bank for Reconstruction and Development / The World Bank. 2010. *The Cost of Adapting to Climate Change for Infrastructure*.

[34] State of New South Wales through Roads and Maritime Services. 2017. *New Dubbo Bridge: Preferred Route Option*.

Available: http://www.rms.nsw.gov.au/projects/western-nsw/dubbo-bridge/index.html

[35] Origin Energy 2017. Sustainability Report 2017.

Available at https://www.originenergy.com.au/content/dam/origin/about/investors-media/annual%20review%202017/FY2017%20Sustainability%20Report.pdf

[36] The City of Parramatta. *The Parramatta River in Flood. Image Supplied*.

[37] United States Department of Homeland Defence, Industrial Control Systems Cyber Emergency Response Team. *Cyber-Attack Against Ukrainian Critical Infrastructure*.

Available at https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[38] The Australian Strategic Policy Institute Limited. 2017. *Cyber Maturity in the Asia-Pacific Region 2017*

[39] Commonwealth of Australia. 2017. *Essential Eight Maturity Model*.

Available at https://www.asd.gov.au/publications/protect/essential-eight-maturity-model.htm

[40] Commonwealth of Australia. 2017. *Australia's Cyber Security Strategy: 2017 Update*