

# QUEENSLAND CRITICAL INFRASTRUCTURE DISASTER RISK ASSESSMENT



© The State of Queensland (Queensland Fire and Emergency Services) 2024.

All Queensland Fire and Emergency Services' material in this document – except Queensland Fire and Emergency Services' logos, any material protected by a trademark, and unless otherwise noted – is licensed under a <https://creativecommons.org/licenses/by/4.0/legalcode>.



Queensland Fire and Emergency Services has undertaken reasonable enquiries to identify material owned by third parties and secure permission for its reproduction. Permission may need to be obtained from third parties to re-use their material.

#### Disclaimer

To the extent possible under applicable law, the material in this document is supplied as-is and as-available, and makes no representations or warranties of any kind whether express, implied, statutory, or otherwise. This includes, without limitation, warranties of title, merchantability, fitness for a particular purpose, non-infringement, absence of latent or other defects, accuracy, or the presence or absence of errors, whether or not known or discoverable. Where disclaimers of warranties are not allowed in full or in part, this disclaimer may not apply. To the extent possible under applicable law, neither the Queensland Government or Queensland Fire and Emergency Services will be liable to you on any legal ground (including, without limitation, negligence) or otherwise for any direct, special, indirect, incidental, consequential, punitive, exemplary, or other losses, costs, expenses, or damages arising out of the use of the material in this document. Where a limitation of liability is not allowed in full or in part, this limitation may not apply.

**Bibliographic reference:** Queensland Fire and Emergency Services, 2024.  
*Queensland Critical Infrastructure Disaster Risk Report*. Queensland Fire and Emergency Services, Brisbane.  
<https://www.disaster.qld.gov.au/qemf/Pages/Assessment-and-plans.aspx>

## Foreword

Critical infrastructure is intertwined into our everyday lives. People depend on the availability of electricity, water, internet and phone service at their homes, and require access to transportation to go to work, school, and just about anywhere else.

Critical infrastructure is also crucial for us all before, during, and after disaster events, for the community generally and the response and recovery agencies working to keep the community safe. Without access to these services, society wouldn't be able to function as it currently does.

The Critical Infrastructure Disaster Risk Assessment (CInDRA) is Queensland's first assessment of climate and disaster risk to critical infrastructure. The assessment recognises the interdependencies between all the critical infrastructure sectors and how the sectors are exposed to different hazards.

Climate change presents ongoing challenges to critical infrastructure, with an increase in the frequency and severity of extreme weather events, and an increased likelihood of multiple events coinciding at the same time, or concurrently. Coastal hazards are also a significant concern for critical infrastructure, with the majority of Queensland's infrastructure and development located within 50km of the coastline.

The CInDRA assesses risk to four critical infrastructure sectors – energy, water, transport and communications. These sectors are recognised as being crucial in the context of disasters, and the interdependencies are complex. Twelve hazards were considered for the assessment – the ten hazards within the



**Nikki Boyd MP**

*Minister for Fire and Disaster Recovery and  
Minister for Corrective Services*



**Steve Smith AFSM**

*Commissioner, Queensland Fire and Emergency Services*

2023 State Disaster Risk Report, along with space weather and cyber security.

These additional hazards highlight the changing landscape of risk, and the growing threat from space weather events, and cyber-attacks targeting critical infrastructure. Space weather can disrupt communication systems, satellite operations and electrical grids, while cybersecurity threats can compromise the integrity, availability and confidentiality of critical infrastructure services.

There are currently significant reforms being led by the federal government to increase the resilience and security of critical infrastructure nationally. Within Queensland, it is important that risks are understood and managed across all levels of Queensland's Disaster Management Arrangements (QDMA). In particular, the risks identified within the CInDRA can assist local and district disaster management groups with understanding the risks to their communities and how to ensure their safety during disaster events.

As the Minister for Fire and Disaster Recovery and Minister for Corrective Services, and the Commissioner of Queensland Fire and Emergency Services, we greatly appreciate the efforts of all stakeholders within QDMA and their

commitment to building safer and more resilient communities. We particularly thank those stakeholders who were involved in the development of the CInDRA, including the owners and operators of critical infrastructure in Queensland. We also acknowledge the ongoing cooperation of local governments, whose collaboration has been instrumental in our collective efforts. Together, we can continue to work towards a safer and more resilient Queensland.



# Executive Summary

## Purpose and Intended Use

The Critical Infrastructure Disaster Risk Assessment (CInDRA) has been developed as a state-level risk assessment, looking at general trends and risks for critical infrastructure. This assessment fits within the suite of state-level risk assessments developed by Queensland Fire and Emergency Services and partners, under the State Disaster Risk Report (SDRR). The assessment is not intended to be detailed and does not provide asset-level risk information. Local or district disaster management groups can use the CInDRA to understand these general risks and how they may manifest at the local, district, or asset level, when conducting a local or district level disaster risk assessment.

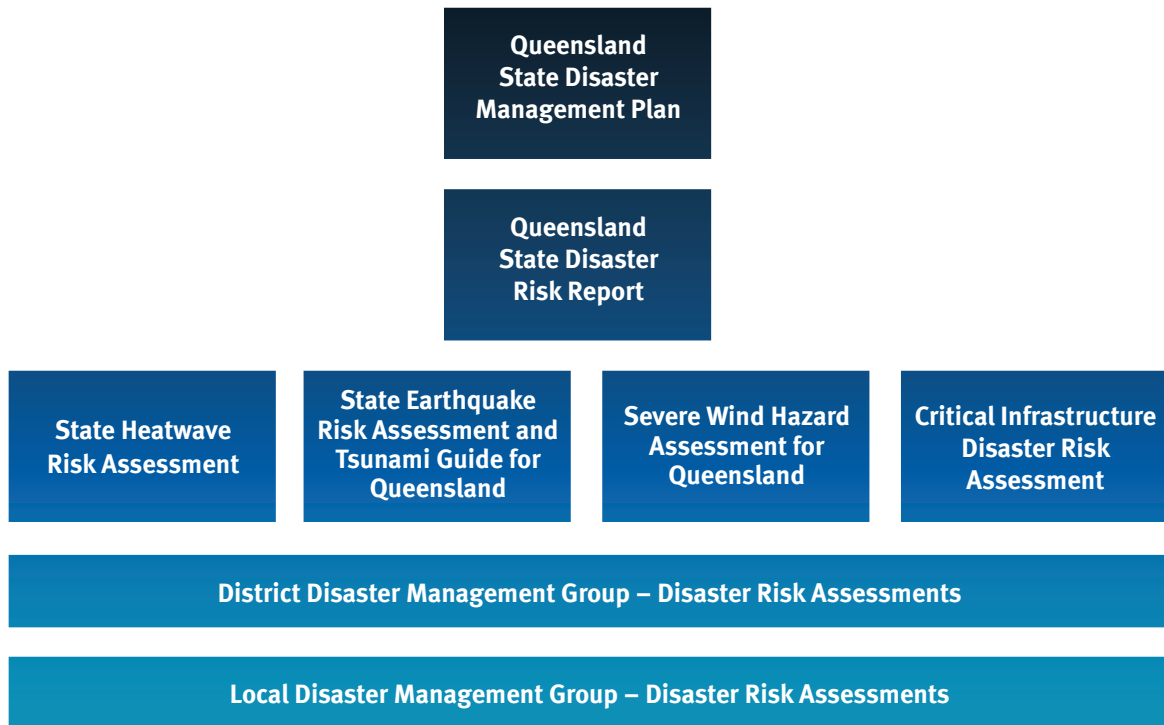


Figure 1: Context of the Critical Infrastructure Disaster Risk Assessment and where it sits with the other state-level hazard and risk assessments for Queensland.

The SDRR and other state-level hazard and risk assessments use the Queensland Emergency Risk Management Framework (QERMF) to assess and prioritise risk. The QERMF is the Queensland Disaster Management Committee’s endorsed approach for disaster and emergency risk management, intended for use by stakeholders within Queensland’s Disaster Management Arrangements (QDMA). Using the QERMF, the CInDRA prioritised risk statements by assessing the vulnerability and consequence of the risks and provided three priority risks for each of the sectors which were assessed in greater detail. These priority risks have been provided as examples for stakeholders within QDMA who may wish to consider critical infrastructure risks within their disaster risk assessments.

While the risks within the assessment may seem easily apparent, this is the first iteration of a state-wide critical infrastructure disaster risk assessment for Queensland. The consideration of risk across the four sectors brings a shared understanding within each sector and across sectors, acknowledging the interdependencies which exacerbate risk. This also highlights opportunities for further research and assessment to advance efforts in critical infrastructure resilience, to improve community outcomes during and after an event.

Iterative approaches to risk assessment and management are necessary to ensure understanding of risk remains current, including regular reviews of risk assessments and disaster management plans. This could include scenario analysis, stress testing, and options analysis, among others, to understand both the anticipated and unanticipated changes to how systems will respond.

As this is the first CInDRA for Queensland, it is intended the assessment will be regularly reviewed and updated to provide new and more detailed information. Future iterations of the CInDRA may consider additional critical infrastructure sectors - such as those listed within the [Security of Critical Infrastructure Act 2018 \(Cth\)](#) (the SOCI Act), with the potential to also provide updates on treatments and implementation of resilience and risk reduction activities across Queensland. It is also intended that as the assessment is updated, information continues to be tailored for users to suit their needs.

## Key Contacts

Further information and advice regarding critical infrastructure risk (for the four sectors within this report) can be sought from:

- Queensland Government Cyber Security Unit: [cybersecurityunit@qld.gov.au](mailto:cybersecurityunit@qld.gov.au)
- Queensland Reconstruction Authority: [hazard.risk@qra.qld.gov.au](mailto:hazard.risk@qra.qld.gov.au)

## General Context

This report delivers a detailed assessment of the climate and disaster risks facing critical infrastructure in Queensland, providing an in-depth analysis which is supplementary to the critical infrastructure failure chapter in the State Disaster Risk Report.

The assessment aligns with the Royal Commission into National Natural Disaster Arrangements recommendation to identify, assess, mitigate and monitor risks to critical infrastructure from natural disasters, and also acknowledges the obligations on the Queensland Government and critical infrastructure owners as a result of the SOCI Act.

### Recommendations 9.4 Collective awareness and mitigation of risks to critical infrastructure

The Australian Government, working with state and territory governments and critical infrastructure operators, should lead a process to:

- 1) identify critical infrastructure
- 2) assess key risks to identified critical infrastructure from natural disasters of national scale or consequence
- 3) identify steps needed to mitigate these risks
- 4) identify steps to make the critical infrastructure more resilient, and
- 5) track achievement against an agreed plan.

This assessment considers risks for four key critical infrastructure sectors (See Figure 2):

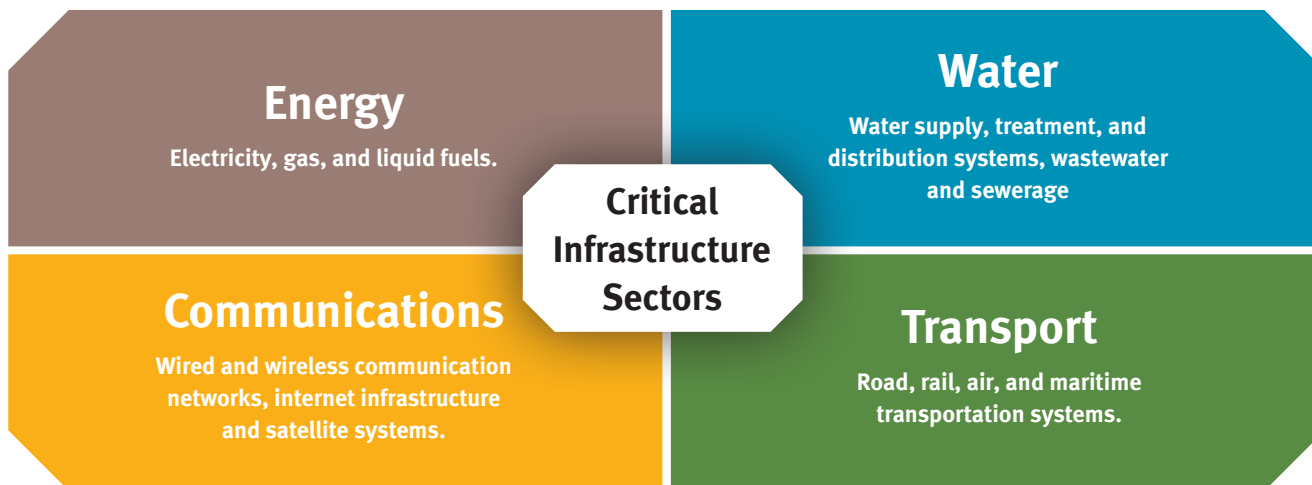













Figure 2. Four critical infrastructure sectors assessed in this report.



These sectors were identified as being the most critical infrastructure for the functioning of a community, with other critical infrastructure also dependent on these four sectors. The hazards assessed in this report include all of the hazards identified in the State Disaster Risk Report, along with two additional hazards: space weather and cybersecurity. The inclusion of space weather and cyber security recognises the increasing interconnectedness of critical infrastructure systems and the growing threat from space weather events, and cyber-attacks targeting critical infrastructure. Space weather can disrupt communication systems, satellite operations and electrical grids, while cybersecurity threats can compromise the integrity, availability and confidentiality of critical infrastructure services. While it is recognised that there are many other hazards which could result in a failure of critical infrastructure, the assessment only considers these twelve hazards:

Table 1. Hazards which have been considered in this assessment.

Hazard	Icon	Hazard	Icon
Heatwave		Tsunami	
Bushfire		Earthquake	
Tropical cyclone		Pandemic	
Flooding		Chemical, Biological, Radiological	
Severe thunderstorm		Biosecurity	
Cybersecurity		Space weather	

The risks identified are based on the current timeframe, however with the influence of climate change and changes in other risk drivers, it is likely these risks will change into the future. For example, in some locations, hazards such as heatwave, bushfire, tropical cyclone, and flooding may increase in intensity and severity, while in other locations the risk from these hazards may decrease.

## Climate Change and Critical Infrastructure

Critical infrastructure will experience challenges from climate change, not just from increased average temperatures, but from the increasing frequency and severity of climate-influenced hazards. The interdependencies of critical infrastructure also mean that impacts to only one sector (e.g. energy) can have knock-on impacts to other sectors which can then cascade through the whole economy.

While critical infrastructure is exposed to climate risks across the state, exposure to coastal hazards is of particular concern, with the majority of Queensland's infrastructure and development located within 50km of the coastline. The areas of most concern include North Queensland, and predominantly, South-East Queensland. This is consistent with the Intergovernmental Panel on Climate Change's (IPCC) identification of South-East Queensland as a 'climate change hotspot' due to the high concentration of population (and infrastructure) in proximity to the coast.

Climate change also increases the likelihood of multiple events coinciding at the same time, or concurrently. The IPCC has projected that cascading, compounding and aggregate impacts will grow due to a concurrent increase in heatwaves, droughts, fires, storms, floods and sea level. This can result in communities becoming more vulnerable, as the impacts are amplified and more complex, and recovery may still be ongoing when the next event impacts. Compound events place increased pressure on

emergency services and other responders, where capacity to respond can be exceeded depending on the number or severity of events. The natural environment will also be severely stressed, limiting the ability to recover before the next event occurs, potentially reducing the environment's ability to protect areas from impacts (e.g. mangroves reducing the impacts of wind and waves along coastlines).

The [Queensland Built Environment and Infrastructure Sector Adaptation Plan](#) (SAP) provides a framework for the sector to plan for and adapt to the impacts of climate change. Released in 2017 (and due to be updated), the SAP acknowledges that the sector recognises climate change as a material risk to business operations in the short and medium term, and that the sector is already undertaking a broad range of activities directed at managing climate risk and building organisational resilience. There are seven Priority Actions identified in the SAP which focus on collaboration within and outside of the sector, risk identification, and information development across the sector. The highest priority action is to:

“Identify incentives to encourage and facilitate the built environment and infrastructure sector to adapt to climate change and to design and build assets to go beyond minimum standard requirements.”

7

This priority action recognises that infrastructure is only built to meet a minimum standard which does not always consider future climate change. By considering climate change within and beyond the expected lifetime of the asset, infrastructure can be safeguarded from projected climate hazards into the future.

## Priority Risks

General risk statements were identified by subject matter experts (government and industry) from each of the sectors during workshops. Scenario analysis was used for each of the hazards assessed, based on data where available. These risk statements are at Appendix A of the assessment.

For Local or District Disaster Management Groups (LDMGs or DDMGs) identifying risks, it may be useful to consider a broader definition of critical infrastructure. For example, the risk assessment may assess the sectors considered within the Essential Utilities category of the QERMF, or it could consider the critical infrastructure sectors identified within the SOCI Act. It will be up to the LDMG/DDMG to determine the most appropriate sectors to assess, relevant to the local area.

Risks were then prioritised in-line with the QERMF, assessing the hazard, vulnerability and consequence through qualitative research and input from industry and government stakeholders through a risk prioritisation workshop. Three priority risks were identified for each sector, as well as for 'All-sector risks', which provide more detail on the vulnerability and consequences of the risk.

The priority risks have not been provided in order within this assessment and are provided as an example of how to consider the hazard, vulnerability and consequence of a risk. As the intention of this assessment is to provide general information and advice to stakeholders within QDMA, it is up to the user to determine how this information could be used within other disaster risk assessments (at the local or district level).



## All Sectors

Timely decision making, compounding events, and cyber security were the priority risks which affected all sectors. It is important to note the complex relationship between sectors and the possibility of compounding effects from one risk to another.



Figure 3. Coronavirus border control measures, Coolangatta, Queensland.

### Priority risks

- A1:** Decision-making of government and infrastructure owners/operators to the event is unclear resulting in a delayed response and increased consequences.
- A7:** Compound and cascading events result in failures of critical infrastructure and extended disruptions.
- A15:** Information systems damage or deliberate cybersecurity attack leads to disruption of critical services resulting in physical and reputational damage, and economic impacts.

## Energy

The priority risks identified for the energy sector were all related to infrastructure damage. Fallen power lines are a risk to community safety, widespread damage would put a strain on generator availability leaving more homes without power, and demand for repairs would increase supply stress resulting in extended outages.





Figure 6. Powerlines damaged by fallen tree during severe storms on the Gold Coast.

### Priority risks

- E6:** Significant damage to the electricity network and fuel infrastructure leads to high demand for replacement parts and difficulties sourcing these parts, resulting in extended power outages.
- E8:** Disaster event impacts a large region and/or multiple jurisdictions, resulting in a lack of generators to service the population required.
- E15:** Strong wind and debris lead to downed powerlines resulting in safety concerns for communities.

## Water

The priority risks for the water sector related to failure of water supply systems and associated infrastructure due to a severe event such as extreme rainfall or an earthquake. The third priority risk was the ability to access critical supplies to restore systems and repair damage.

### Priority risks

- W8:** Extreme (or constant) rainfall leads to inundation of water treatment facilities resulting in failure of water supply systems.
- W9:** Earthquake compromises the structural integrity of water storages resulting in failure of infrastructure and potential inundation of surrounding communities.
- W13:** Ability to access critical supplies (e.g. spare components, chemicals, fuel) impacted.



## Transport

Priority risks for the transport sector relate to disruption to services resulting from power outages, causing delays and concerns to safety, damage to rail and road infrastructure and the costs associated to repair, and cyber-attacks that will impact control and community safety.

### Priority risks

- T1:** Power outages result in disruptions to service availability (particularly for trains).
- T2:** Power outages lead to signalling issues, resulting in traffic congestion and safety concerns (road).
- T6:** Flooding leads to damage or destruction to roads or rail resulting in increased repair and maintenance costs.
- T21:** Cyber-attack leads to operational technology disruptions resulting in significant safety concerns for customers using transport systems (public transport, signalling, and signage), and economic impacts due to disruptions to freight and shipping systems.

10



Figure 7. Flooded creek damaging roadway – Ex-TC Debbie, March 2017



Figure 8. Flooding at Macrossan Bridge over the Burdekin River, near Charters Towers, Feb 2019

## Communications

Priority risks for the communication sector identified that the main concerns were for disruption to networks such as NBN and mobile communication, with a significant risk to safety and communication for responders. The third priority risk was the inability to deploy temporary telecommunication facilities due to access issues or evacuation orders.

### Priority risks

- C4:** Power disruptions result in outages of NBN (impacting community safety and disrupting essential services).
- C5:** Power disruptions result in loss of mobile communications (impacting community safety, emergency services, emergency alerts, etc.).
- C6:** Deployment of temporary telecommunications facilities, such as Cells on Wheels are not able to be deployed due to road access issues, evacuation orders, movement restrictions, or other technical restriction.

## Treatments and next steps

The treatments below have been identified through desktop research and discussion with government and industry stakeholders. Many of the treatments listed are already implemented as business-as-usual risk management practice, while other treatments are provided as potential 'next steps' in risk management.

- Business continuity planning, focusing on working collaboratively with other owners/operators.
  - › BCPs are frequently prepared by CI owners/operators, and these plans are generally robust. However, BCPs should be prepared to address vulnerabilities to, and prepare for consequences of, compounding and cascading events. Additionally, harmonisation of BCPs with whole-of-sector and cross-sector input will strengthen each agency's ability to mitigate disaster risk and respond to disaster events. State and Local Governments should also have robust BCPs in place which account for disruption to CI.
- Development of training programs for staff. Training is essential to ensure general knowledge of disaster risk, Queensland's disaster management arrangements, and how CI owners/operators fit in these arrangements.
- Data-sharing with government and infrastructure owners/operators to facilitate accurate risk assessments, intelligence products, and risk reduction effort during all phases of disaster management (PPRR). These data may pertain to assets, services, and the status of the network.
- Undertaking exercises with broad participation from the CI sector will strengthen general knowledge of response to disaster events. Particularly, roles during response can be defined, and BCPs can be stress tested.
- Committees or groups, with a meeting rhythm aligned to the disaster season. This will allow for the coordination of planning and response. Creating connections between CI owners/operators, government, and the broader community will strengthen response to events, particularly in the case of compounding and cascading events.
- Investment for further research in understanding hazards, including compound and cascading events, and other hazards which may not have been subject to extensive research efforts thus far. This may include enhancing early warning and predictive modelling for these kinds of events.
- Investment in building cybersecurity capability for each agency (and government), ensuring that management of these risks respond to obligations under the SOCI Act.
- Coordinate generator and fuel inventory with other CI owners/operators and local government. Memorandums of Understanding or agreements for resource sharing as needed during events should be developed through Local or District Disaster Management Groups, or sector-led groups where these may already be in place.
- Investment in increased local manufacturing capacity, with a focus on diversifying supply across jurisdictions. This should include investment in building a skilled workforce, and strengthening the representation of women, people with disabilities, and First Nations peoples in the industry.
- Continued development of new technology, including more resilient infrastructure and an increase in uptake of renewable energy systems (including standalone power systems and other strategic battery systems).
- Replacement programs for assets which exceeds minimum or 'last-event' standards. This could include increased wind loading standards, infrastructure that can withstand higher temperatures, or bridges/roads replaced at a greater height to withstand flooding.
- Investment in more resilient road infrastructure at priority locations to maintain connectivity for freight and access to communities and for repairs.
- Real-time monitoring systems to detect impacted assets with automatic shutdown. This prevents further asset damage and increases community safety.
- Community education and information messaging to inform the community of safety risks and increase personal resilience.
- Multiple lines of communication (satellite, radio, etc.) to enhance redundancy in the case of power or communication outages.
- Regular inspection and maintenance programs to ensure infrastructure is secure and functioning as expected.
- Effective planning and risk assessments conducted for asset sites to minimise exposure to a hazard.



- Adequate stockpile of critical supplies, ensuring that this stockpile is consistently maintained so repairs can be made easily during times of crisis.
- Increase cross agency collaboration to:
  - › develop agreements and priority response mechanisms to support the functioning of other reliant critical infrastructure during disaster events.
  - › Improve awareness of roles and responsibilities.
  - › Expedite response to community during disaster events.

The treatments listed above are examples of best practice risk management, aimed at reducing risk to critical infrastructure and to the community. There are varying levels of risk maturity across the critical infrastructure sectors, and across regions in Queensland. Many organisations have already implemented or begun implementing some of these treatments into their work to minimise the impacts caused by climate change and other hazards. Some organisations may still be at the risk identification stage and are focused on the initial development of a risk management program, to ensure compliance with the SOCI Act.

The [Queensland Strategy for Disaster Resilience](#) recognises the need for resilient critical infrastructure, with success of Objective 2 dependent on the “reliable and continuous operation of critical infrastructure despite the stresses or shocks that may occur.”<sup>63</sup> This Objective requires the coordination and collaboration of stakeholders across industry and government to address the cross-cutting consequences of climate and disaster risk. As seen throughout this assessment, several risks and treatments are applicable across multiple sectors. The development of sector specific resilience strategies or action plans, aligned with the Queensland Strategy for Disaster Resilience, may be a beneficial means of facilitating collaboration and achieving better outcomes than organisations working in silos.

While this assessment only considers risks to four critical infrastructure sectors, there are multiple other sectors that provide critical infrastructure to Queensland communities. The Critical Infrastructure Disaster Risk Assessment is Queensland’s first state level risk assessment for disaster risks to critical infrastructure. Future iterations of this assessment have the potential to consider additional sector risks, building on the state’s knowledge and understanding of the impacts to communities when critical infrastructure fails, and how the sector is continuing to work on increasing resilience to these hazards.



