



## Risk Assessment Advisory for Critical Infrastructure Communications Sector

The international and domestic threat landscapes continue to evolve; natural hazards are becoming more prevalent, with longer-lasting impacts and, critical infrastructure networks continue to be targeted globally by both state and criminal cyber actors. As a result, stakeholders within Australia's Communications Sector must adapt their risk management strategies to ensure risks to the operation of assets critical to the nation's economic and social wellbeing are being appropriately captured.

This material has been designed to provide guidance on assessing these types of risks to Australia's critical infrastructure. Through the provision of suggested risk assessment approaches, the material aims to assist sector stakeholders to adapt existing risk practices and help organisations understand risks within the broader national critical infrastructure context. The document comprises the following sections:



Risk in the critical infrastructure context



Determining criticality of assets



Interdependencies (upstream and downstream)



Understanding threats and hazards for risk



Risk controls and mitigations



A risk assessment methodology

Some features of risks in the **Communications Sector** are outlined below:

**An essential service** – relied upon by the Australian society and economy to communicate, collaborate, and operate within our digital world.

**Highly regulated sector** – telecommunications as a sub-sector is already regulated by the CISC in a national security context.

**High reliance on physical assets including some in remote areas** – susceptible to natural disasters

**High value target** – potentially targeted by nation-state actors due to the criticality of the sector for society's everyday life, and our national security.

**Geographically distributed infrastructure** – widely distributed geographic locations across Australia.

**Vulnerable supply chain** – susceptible to attacks launched through third-party hardware and software used by telecommunications providers. Upstream, it is also dependent on the Energy Sector, particularly in remote locations.

**Supportive of critical and emergency services** – inclusive of 000, .au domain holders, and connected biomedical equipment.



## Risk in the critical infrastructure context

### Identifying risk for critical infrastructure

Risk in the context of critical infrastructure is related to Australia's national and societal resilience. This may differ from the way entities have viewed risk in the past (for example, with financial or shareholding interests as a focal point). Risks that have the greatest impact on the social or economic stability of Australia or its people, the defence of Australia or national security, also need to be considered and framed within critical infrastructure entities' existing risk management strategies.

An example of how to identify this risk for the Communications Sector is framing a possible risk from the supply of a faulty component from an unreliable or high-risk vendor hardware provider, disrupting the availability of the asset if the faulty component was integral to the asset's operational capability.

### Taking an all-hazards approach to risk.

For critical infrastructure organisations, an all-hazards approach to determining risk is recommended. All-hazards is an integrated approach to risk management, preparedness and planning that focuses on businesses enhancing their capacities and capabilities across a full spectrum of threats and hazards to Australia's critical infrastructure.

All-hazards risk assessment considers both threats (human-induced) and natural and environmental hazards that could impact on a critical infrastructure entity and its operations. Australia's critical infrastructure risk environment continues to evolve and an all-hazards approach is best placed to consider the potential converging of the wide-ranging threats and natural hazards it confronts, which could result in multiple and cascading effects on national resilience.

Critical infrastructure organisations are uniquely positioned to assess to critical infrastructure risk through the analysis of those identified threats and hazards to their sector against their own assessment of vulnerabilities. As part of this risk identification, organisations can consider broadly how the *confidentiality, availability, integrity* and *reliability* of their assets may be impacted during and after any incident.

Understanding this potential 'relevant impact' is important to prioritise risk and determine how best to both minimise the likelihood of the risk occurring and mitigate the potential impact. Examples of how these relevant impacts can be applied for assets in the Communications Sector has been provided in the **Understanding sector-specific risks** section of this document.

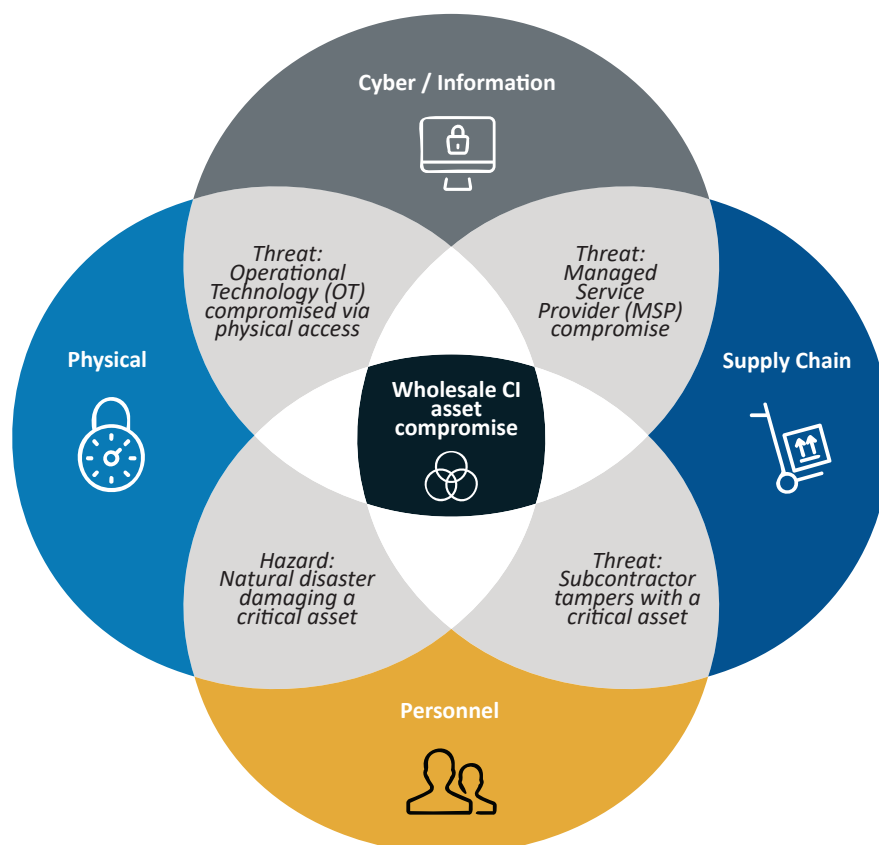
Some entities in the Communications Sector have security-related regulations already in place. Entities in the sector may need to consider guidance such as the Telecommunication Sector Security Reforms (TSSR), or look to their state or territory governments for regulatory frameworks and consider how they can incorporate national security-related risk into existing risk management frameworks. Entities should also refer to other CISC sector guidance for further information.

### Convergence risk

Australia's adversaries pose an increasingly sophisticated threat to our critical infrastructure and often look to exploit multiple vulnerabilities via multiple vectors in unison. Sector-wide convergence risks eventuate due to interdependencies within and across critical infrastructure sectors, as well as through other links, such as supply chain relationships. Furthermore, convergence risks could exist within organisation due in part to internal silos or lack of integration of risk management capabilities.

Adopting an all-hazards risk management approach is a strategy to combat convergence risks and ensure responses are comprehensive and integrated. This requires collaboration between all stakeholders, including internal business units, sector and supply chain stakeholders, law enforcement and emergency services. Organisations should leverage information from government stakeholders to appropriately consider appropriate threats and hazards. Adopting multidisciplinary approaches, collaboration and integration is a good approach for inclusion in a critical infrastructure entity's risk assessment. The following diagram illustrates an example of how a convergence threats can be represented as risk.

Figure 1. Examples of converging threat and hazard on risk identification





## Determining criticality of assets



### *Security of Critical Infrastructure Act 2018 (SOCI Act) – Section 5:*

Communications Sector means the sector of the Australian economy that involves:

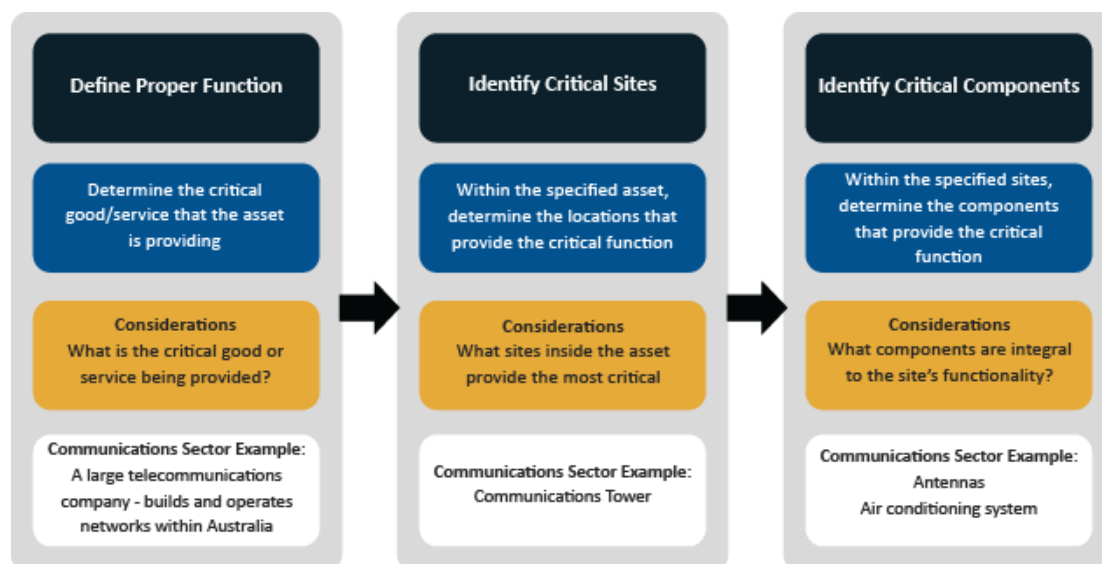
- (a) supplying a carriage service; or
- (b) providing a broadcasting service; or
- (c) owning or operating assets that are used in connection with the supply of a carriage service; or
- (d) owning or operating assets that are used in connection with the transmission of a broadcasting service; or
- (e) administering an Australian domain name system

### Identifying and assessing criticality

For Communications Sector critical infrastructure providers, determining which sites and components of an asset should be considered critical involves identification and analysis of how an asset and its operations may be exposed to, or harmed by, threats and/or hazards. This process is vital for all hazards risk management, providing input into the identification of plausible risk scenarios that may impact operations. The critical sites and components of an asset are ultimately those most vital to its effective functioning and therefore integral to Australia's national security interests. Establishing criticality is designed to provide guidance on the allocation of resources to best protect the operational capability of the asset.

The 'responsible entity' for an asset is able to determine the extent of this activity; however, a suggested process using a select example is outlined below.

Figure 2. Example of determining criticality of an asset





A function of a critical infrastructure asset may be the provision of a critical good or service that is a contributor to the economic or social wellbeing, defence, or security of the nation.

For example, a large Australian service provider has been identified as critical as its mobile network covers more than 23 million Australians. The proper function of this asset may be compromised if it is unable to deliver mobile and fixed broadband services to its customer base.

Critical sites are those in which assets assigned proper functions are located. This could include 5G towers, DNS server rooms or other areas based on the context of the specific asset. It is important to identify if the asset is networked, standalone, or non-networked to appreciate the level of criticality.

The responsible entity of a critical infrastructure asset is required to do what is 'reasonably practicable' to minimise and mitigate risk associated with critical components. This means that entities must also identify critical components.

Critical components are those required to maintain the function of the asset, or whose absence, damage or compromise could cause significant damage to the asset. For a communications organisation, critical components may include a dish antenna that is used to receive or transmit information by radio waves to or from a communication satellite, or a transmitter that produces radio waves in order to transmit data.



## Analysis of emerging trends and technologies

Identifying important trends and technology drivers and how they impact risk can be challenging; trends interact in unpredictable ways, with at times profound consequences. The following key trends and technologies have been identified as potential domestic changes that could impact on risk in the Communications Sector:

Figure 3. A selection of emerging trends and technology that can impact on risk in the sector

### Emerging Trends

- **Increased self-sufficiency:** Telecommunications providers are reducing their reliance on energy providers by integrating their own power generation and transmission infrastructure into their existing networks. These changes often include adding infrastructure such as solar panels, generators, and uninterruptable power supplies to meeting internal needs and reduce energy-sector dependency.
- **Internet access as a human right:** The Australian Human Rights Commission wrote: “has been argued at the international level that such access is critical, particularly in terms of the right to freedom of expression, and in the redressing of structural disadvantage”. This is likely to increase pressure on communications providers to provide accessible, high quality, and widely available services to all users, including those in remote locations.
- **Rapid changes in communication needs:** As demonstrated in the move to online working and online educating that was necessitated by the COVID-19 pandemic. Long-practised ways of working may continue to shift, necessitating further scalability planning.
- **The need to reassess cybersecurity and risk management in the 5G era:** While the widespread adoption of 5G offers many benefits, it also creates new security concerns and challenges.
- **Increasing ubiquity of online platforms:** A key development within sector has been the rise of internet platforms and intermediaries are firms that provide or facilitate transactions between third parties over the internet, thereby creating value through connecting users on a shared platform and capturing value through charging for access.
- **More diverse viewing patterns:** The demand for mobility and growth in the range of content is affecting Australian viewing patterns. Consumers are increasingly able to shape their own viewing experiences, choosing what, when and where they consume media.

### Emerging Technology

- **Enabling the forth revolution in communications technology innovation:** Deploying substrate blockchain technologies, such as 4G, 5G, and the National Broadband Network (NBN), into existing infrastructure across Australia and helping other sector and industries innovate.
- **Increasing need for high-capacity wireless communications:** Including in remote areas where technology integration and high demands for communications capacity and availability continues to increase.
- **Rising interest in multi-access edge computing and private cellular networks:** The enterprise market for private cellular networks and edge computing is gaining momentum. Network operators will have to compete against other player, who may prove key partners in delivering their solutions.
- **Emergence of over-the-top (OTT) services:** OTT refers to applications and services that are accessible over the internet, without any direct influence or control from network operators or internet service providers (i.e. Netflix).



## Sharing national security risk information with government

The Australian Government's national intelligence community collects and analyses information to constantly monitor, assess and provide advice on threats to Australia. Much of this information is classified and not made available to the general public; however, as part of their mandate the following portals provide open source information, assessments and advice designed to support critical infrastructure sectors.

Organisations are able to contribute to the process of monitoring and assessing threats through internal risk assessments. By identifying emerging risks, organisations are able not only to directly improve their security stance but share this information with external security bodies. The following organisations are able to receive threat information, distributing threat awareness across the sector:



CYBER AND  
INFRASTRUCTURE SECURITY  
CENTRE

### Trusted Information Sharing Network (TISN)

A set of bodies of industry and government representatives that meet to share information on issues relevant to the resilience of critical infrastructure and the continuity of essential services in the face of all hazards.

For further information on TISN and how to join the network, please go to:  
<https://www.cisc.gov.au/engagement/trusted-information-sharing-network>



ACSC Australian  
Cyber Security  
Centre

### Australian Cyber Security Centre (ACSC)

A hub for private and public sector collaboration and information sharing on cyber security. to prevent and combat threats and minimise harm to Australians.

To engage with the ACSC, fellow partners, and help uplift cyber resilience across the Australian economy, join the ACSC partnership program here:  
<https://www.cyber.gov.au/partner-hub/acsc-partnership-program>



### Australian Security Intelligence Organisation (ASIO) Outreach

Provides advice to government, industry and academia on current and emerging security threats.

To register to the Outreach program and gain access to security updates, please go to:  
<https://www.outreach.asio.gov.au/>



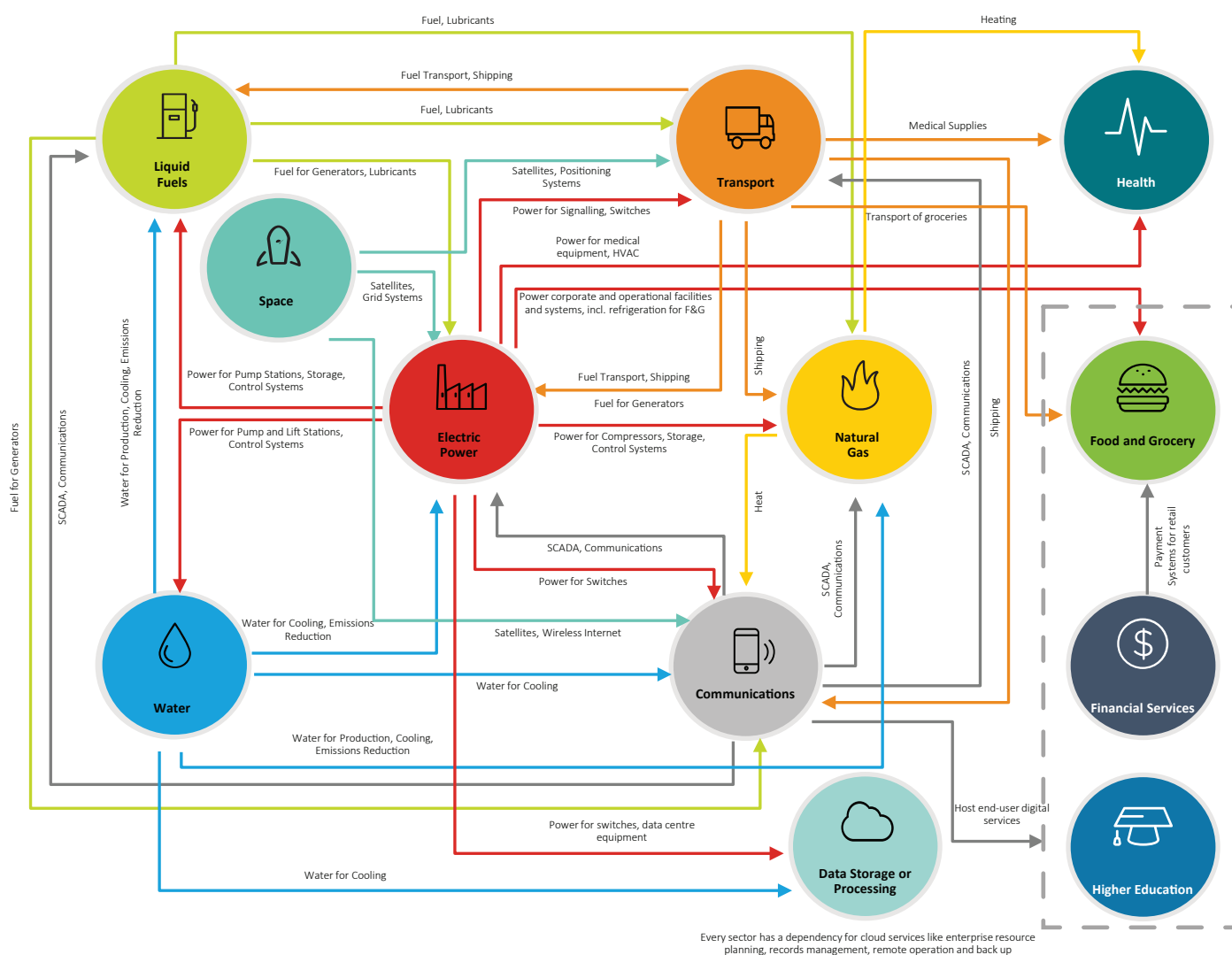
## Interdependencies (upstream and downstream)

### Sector interdependencies and relationships

Because critical functions can be exposed and vulnerable in the event of failure within another critical infrastructure sector, a critical infrastructure entity needs to carefully consider the sector interdependencies that interact with its operations as part of any critical infrastructure risk assessment.

The Communications Sector is an upstream dependency of a number of other critical infrastructure sectors; as much as other sectors rely on its downstream services. The following diagram provides one example of the explicit connections and dependencies, both upstream and downstream, that extend across critical infrastructure sectors.

Figure 4. An example of sector interdependencies and relationships

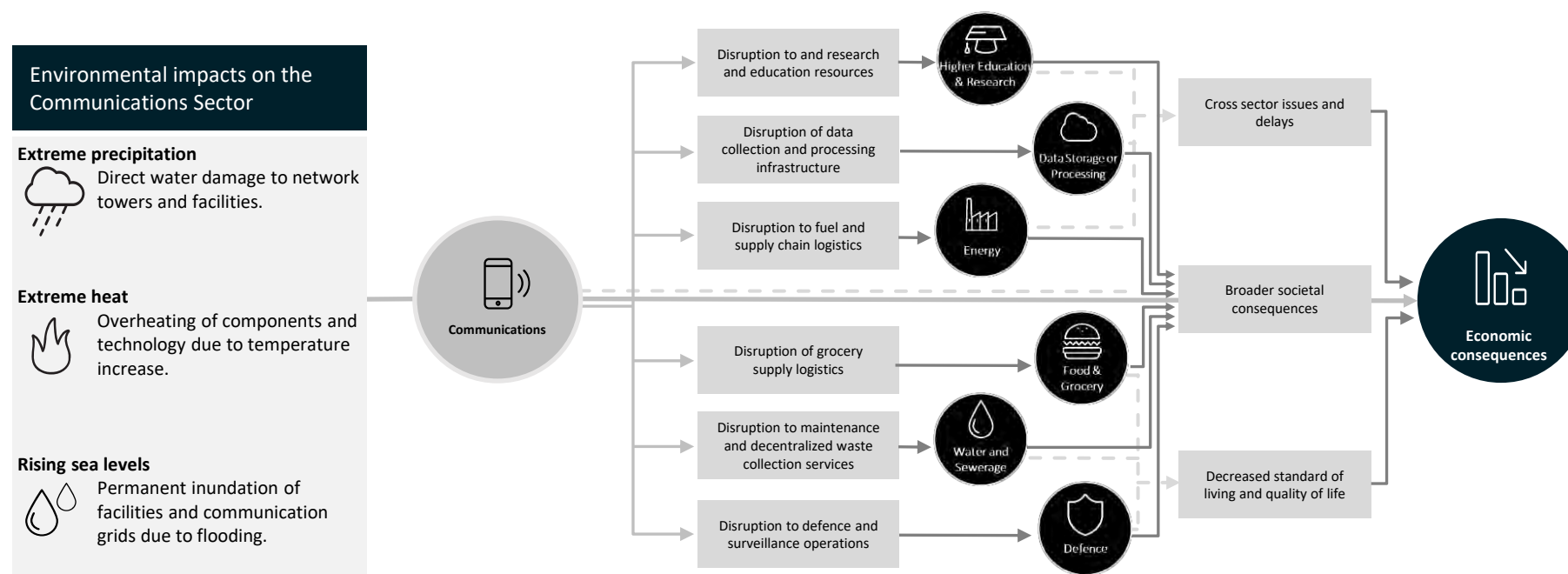




## Flow-on effects for relevant impacts against Communications Sector assets

The following diagram illustrates an example of the potential flow on effects to other interdependent critical infrastructure sectors following an impact from a possible threat or hazard event on the Communications Sector.

Figure 5. Example of flow-on effects from an impact against the Communications Sector





An outage affecting a critical asset in the Communications Sector could have substantial economic or societal implications. Impacts could be significant in severity, depending on the geographic breadth of the outage and the extent of the effect on the broader network, and could result in financial, loss of life, and/or reputational impacts ranging from financial penalties to sustained communications interruptions. For example:

- Outages to telecommunications systems creates a tangible impact to health and safety where communications for emergency services are unavailable
- Outages to broadcasting services could prevent important communication to the public during an emergency incident, such as bushfire or flood. Compromise of a broadcasting system could disseminate misinformation to an unwitting public as part of a campaign undertaken by a malicious actor
- Without DNS, or due to a DNS compromise, internet users may be unable to access the websites they are looking for and/or could be routed to malicious sites, or not connected at all, leading to losses in productivity or availability of government or critical infrastructure internet services
- Outages to telecommunications networks can have flow-on effects for banks processing payments for retail; in 2019, an outage that occurred to a NSW telecommunications network is estimated to have cost retailers AUD100 million
- Well-resourced nation state actors could target undersea cables or submarine cable landing stations that connect Australia to the rest of the world
- Remote access to operational technology and industrial control system devices controlling critical infrastructure could be affected by an outage to communications infrastructure
- Communications infrastructure providers could, as a result of any service impacts to clients, be subject to financial penalties or litigation undertaken by customers.

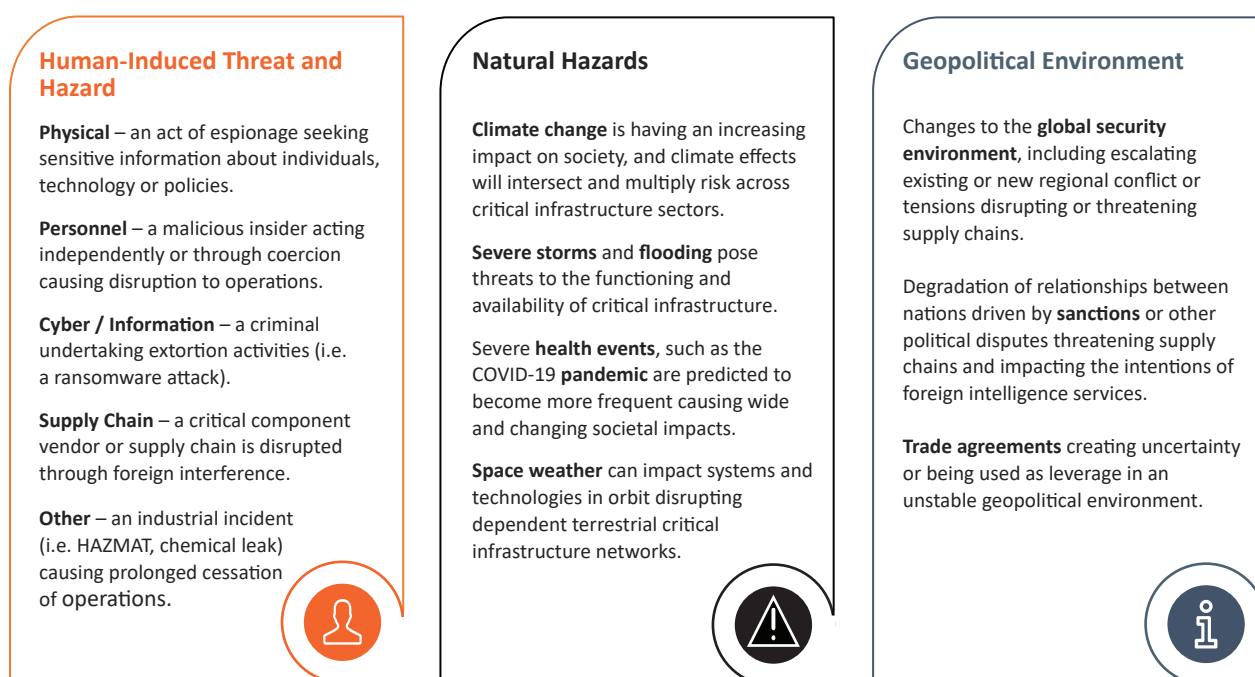


## Understanding threats and hazards for risk

### Identifying a threat and hazard landscape of the Communications Sector

All-hazards risk assessment considers both human-induced and natural threats and hazards. Given its role in critical infrastructure, as well as the key economic importance of its services; the Communications Sector is an attractive target, and the nationally-dispersed nature of its assets increase its susceptibility to natural hazards. A strategic representation of a threat and hazard landscape to a critical infrastructure sector could be structured as follows:

Figure 6. A representation of a threat and hazard landscape to critical infrastructure



It is essential to maintain a broad view of all-hazards risk and management activities for critical infrastructure that covers cyber/information, physical, natural, personnel and supply chain security, to continually monitor for likely threats and hazards.

The nature of physical, personnel, cyber, and supply chain threats to the sector is increasingly sophisticated and well resourced, and the frequency and magnitude of attacks is escalating. Additional considerations might include geopolitical tensions, pandemics, and the demonstrated potential for cyber technologies to be used as a long-distance act of aggression by nation states or other actors.



Threats will increase and the Communications Sector, driven by improvements in technology and the need to meet commercial outcomes, will become more interconnected. This means that stakeholders in the Communications Sector need to reevaluate risks regularly.

Natural hazards are becoming more frequent and intense, their impacts long and complex. The Communications Sector is not immune, as demonstrated in the 2019–20 bushfires that directly affected many telecommunications facilities across the country.






## Understanding sector-specific risks

This table outlines a select example of identified threat and hazard vectors that impact Communications Sector assets. When identifying risk in a critical infrastructure, each threat or hazard vector should be considered alongside the areas of an entity's operation it may potentially impact to allow for a more impact-led determination of plausible risk scenarios to assess.

	Threat or Hazard Vector	Area of Potential Impact	Risk Scenario Considerations
 CYBER / INFORMATION	Foreign interference	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Countries seeking to disrupt Australia's critical infrastructure may use advanced persistent threats or other modus operandi to scope, exert influence and disable communication networks to create disruption or cessation of communication and data services.
	Cyber-espionage	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Cyber espionage could be used to exfiltrate, monitor, intercept and manipulate data pertaining to communication networks and, current and future capabilities.
	Remote access to operational technology	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Remote technology is often used to access interface between an asset's IT and Operational Technology (OT) systems. This can be exploited by malicious actors to gain quick and easy access to critical systems.
	Cyber sabotage	<ul style="list-style-type: none"> <li>Integrity</li> <li>Availability</li> </ul>	If harnessed effectively, cyber attacks can be used to inform cyber sabotage attacks, to gain control of OT, indefinitely suspend or otherwise degrade network capability.
	Financially-motivated cyber-crime	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Ransomware deployed into the networks of communication providers has the potential to halt the functioning of an asset for extended periods with the intent to extract financial benefits.
 NATURAL	Severe weather events	<ul style="list-style-type: none"> <li>Availability</li> <li>Reliability</li> </ul>	Communications infrastructure is likely to be impacted by more frequent extreme weather and natural disasters, causing damage to critical communication network equipment.
	Space weather event	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Availability</li> <li>Reliability</li> </ul>	Geomagnetic storms from space weather events could impact power used to run communication assets or damage electronic equipment via electromagnetic pulses. Additionally, communications infrastructure can be disabled through damage caused to general and GPS satellites in orbit.

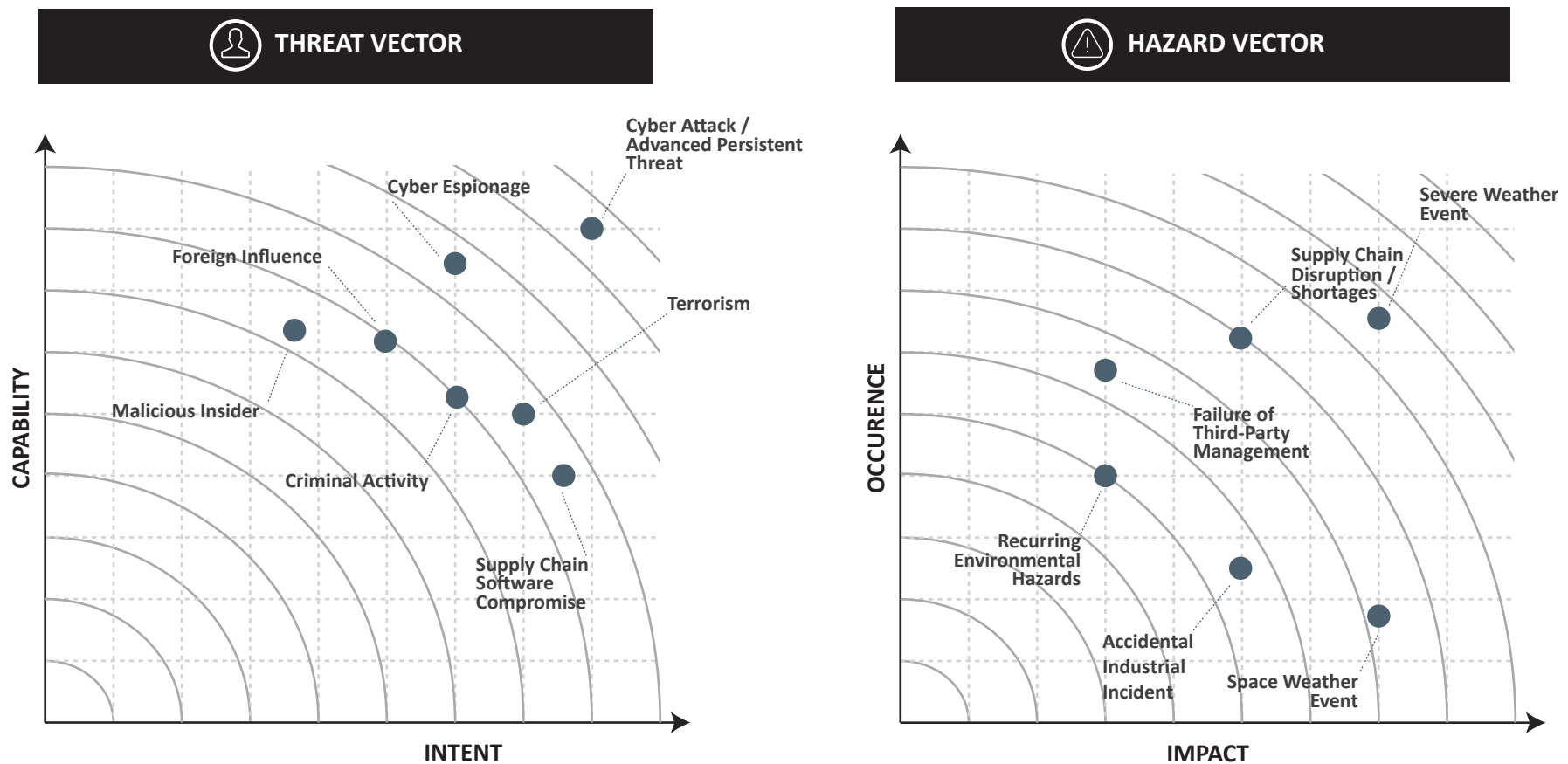


	Threat or Hazard Vector	Area of Potential Impact	Risk Scenario Considerations
 PHYSICAL	Foreign Interference	<ul style="list-style-type: none"><li>Confidentiality</li><li>Availability</li><li>Reliability</li></ul>	Foreign ownership in Australia's communication networks may be subject to interference from foreign adversaries, using access or coercion to gain access to networks or to transmitted and stored data.
	Terrorism	<ul style="list-style-type: none"><li>Confidentiality</li><li>Availability</li><li>Reliability</li></ul>	Groups that seek to make political statements through unlawful means may intentionally damage cell towers, cell grids and wider networks to cause civil unrest.
 SUPPLY CHAIN	Supply issues/shortages	<ul style="list-style-type: none"><li>Confidentiality</li><li>Availability</li><li>Reliability</li></ul>	With many organisations relying on commercially available components to function, shortages of these parts are able to directly affect the functioning of communication assets.
	Failure of third-party management	<ul style="list-style-type: none"><li>Availability</li><li>Integrity</li><li>Reliability</li></ul>	Parts provided by foreign may be affected by international sanctions, and even if components are available Australian communication entities may not be able to purchase needed components.
	Foreign Interference in supply chain by extra-judicial actions	<ul style="list-style-type: none"><li>Confidentiality</li><li>Integrity</li><li>Reliability</li></ul>	Parts sourced from overseas may be subject to interference from foreign adversaries, which could include sabotaged or manipulated components that enable threat access to critical infrastructure in Australia.
 PERSONNEL	Malicious Insider	<ul style="list-style-type: none"><li>Confidentiality</li><li>Integrity</li><li>Availability</li><li>Reliability</li></ul>	A trusted insider has the ability to cause significant damage to critical infrastructure such as deliberately disclosing privileged information or manipulating technology used by assets with the intent to cause harm.
	Accidental industrial incident	<ul style="list-style-type: none"><li>Integrity</li><li>Availability</li><li>Reliability</li></ul>	Hazards, such as an accidental industrial incident can cause significant risk for a entity. For the Communications Sector, an incident such as damage during network maintenance could resulting in a widespread network failure.

## Prioritisation of sector threats and hazards

Organisations will need to form their own view on the threats most relevant to their operations. The following diagram provides a suggested approach to considering the prioritisation of threat and hazard vectors to the sector, by mapping them against intent and capability (threat) and, impact and occurrence (hazards). Understanding this prioritisation of threat and hazards is a key input to assessing levels of risk likelihood.

Figure 7. A representation of prioritisation of threat and hazard vectors



Source: Deloitte Risk Advisory and Cyber and Infrastructure Security Centre



## Risk controls and mitigations

Due to interdependencies among different critical infrastructure sectors and assets, it is necessary to manage many risks collectively. Many risks may be poorly addressed because their causes or effects are still misunderstood, they are novel, or there is a lack of guidance on how to address them. Accountabilities for addressing some risks may also be unclear. Some risks may be too rare to justify allocation of resources to mitigate them. Finally, the consequences may be too large for any entity to address by itself.

For a given Communications Sector asset, the disablement of its resources will cause issues downstream issues in other sectors that are potentially vast and more detrimental to other industries than the direct damages to the asset.

Ongoing analysis of risks can lead to a better understanding of mitigation strategies, including their application at the source.

Business continuity planning, consequence management, emergency management, disaster mitigation, vulnerability assessment, insurance and other related disciplines all provide a variety of possible actions.

Once controls and mitigations options have been identified by an entity, these should be continually evaluated and prioritised, particularly as threats and vectors evolve. The following criteria can be used for development of an implementation plan for risk controls and mitigations:

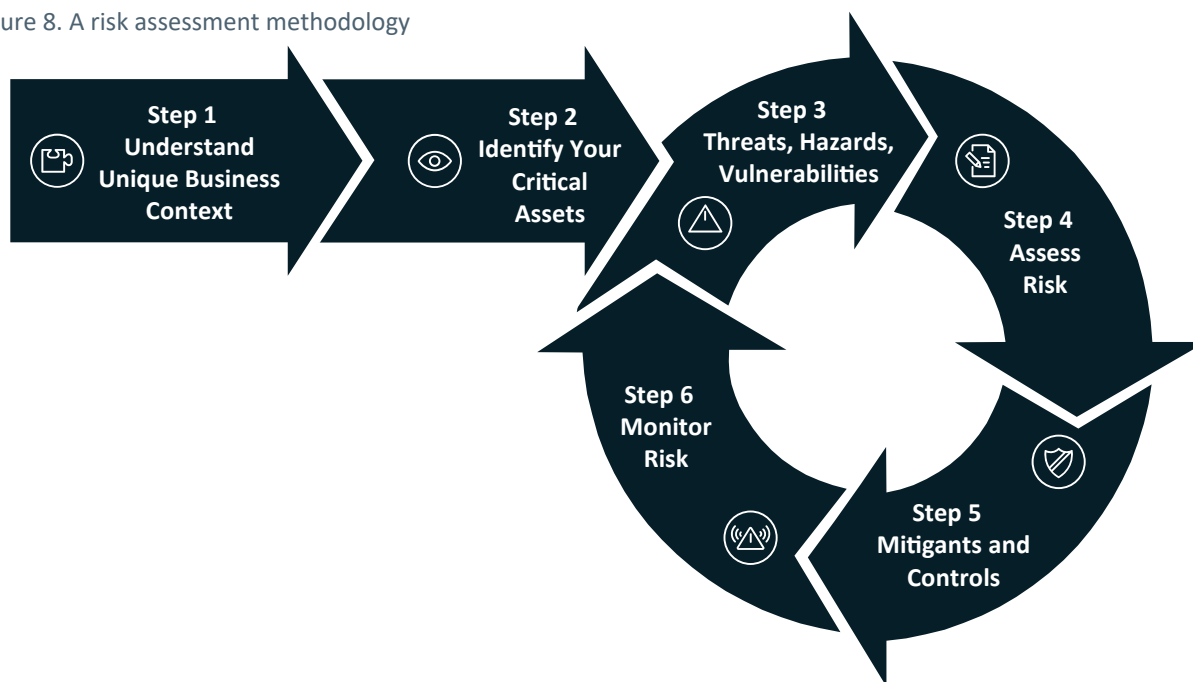
- Ease of implementation
- Cost-effectiveness
- Whether the action creates new risks and/or unintended consequences
- Environmental impacts (positive and negative)
- Multi-objective actions
- Long-term and short-term results
- Effectiveness
- Direct and indirect benefits
- Legal, regulatory, social and moral obligations
- Efficiency
- Equity and acceptability
- Timing and duration.



## Appendix – A risk assessment methodology

Communications Sector organisations looking to improve their risk management processes may want to consider this six-step approach to risk assessment, developed specifically to cater for critical infrastructure assets:

Figure 8. A risk assessment methodology



### STEP 1 – Understand business and sector landscape and how it fits under critical infrastructure

Identify the context of your individual organisation within both the Communications Sector and the Australian economy. Articulate your business objectives, identify your business threats, and understand the security regulations and legislative requirements that you need to follow. There is no one-size-fits-all approach for risk assessment and management. Organisations will need to determine how best to minimise and mitigate risk.

**Outcome** – Understand operational context for your business.





## STEP 2 – Identify your critical assets

Identify what you need to protect. What is valuable to you? Which services, assets and components if disrupted, damaged, or destroyed would adversely impact what is valuable to you? These are your critical assets. Consider: systems, services, networks, people, data, information, and other key elements. Identify dependencies and interdependencies.

Determine what is required for the continuing function of your 'critical infrastructure asset'. What are the key sites and components required to achieve the function of your asset? Components include systems, services, networks, information.

**Outcome** – Determine critical sites, components and personnel required to operate your critical infrastructure asset.

## STEP 3 – Threats, hazards and vulnerabilities

Analyse the threats and hazards that are likely to cause harm to identified critical infrastructure assets. Include consideration of known vulnerabilities that might impact assets, as well as information from the sector more broadly on similar organisations that have been targeted and how this was done. This can also include analysis of threat actors, their motivations and how they might gain access to and attack those assets (who, why and how).

**Outcome** – Identify the most relevant threats and hazards for your particular organisation.

## STEP 4 – Assess risk

Evaluate the risk that each threat poses. How likely is it that the threat might eventuate? What are the potential consequences if the threat is realised? Analyse existing controls that might reduce the likelihood and/or consequence of a security incident. Consider intent and capability for threats, and likelihood and consequence for hazards such as natural disasters.

**Outcome** – Identify risks relevant to your organisation that are likely to impact the confidentiality, integrity, availability or reliability of your critical infrastructure assets.

## STEP 5 – Identify mitigations and implement controls

Decide if the initial outcome of each risk is within a tolerable level, or if additional controls should be implemented. Implement the necessary controls and then update the risk profile (with altered control descriptions, likelihood and/or consequence). Controls might include technology controls, physical controls and/or activities across the spectrum of prevention, protection, detection, mitigation, response, and recovery.

**Outcome** – Treat identified risks as much as 'practicably possible'.



## STEP 6 – Monitor risk

Effective risk management is never a point-in-time exercise; it needs to be ongoing to cater for ever-evolving threats and changing assets and infrastructure that organisations need to protect. Use metrics to measure progress and effectiveness of security risk management activities, supported by appropriate governance arrangements. Undertake continuous improvement measures to harden critical asset vulnerabilities through activities such as red-teaming, post-incident review, and continuous assurance activities. Ensure the outcomes of these activities are used to regularly update and improve the existing spectrum of risk management practices. Maintain a positive security culture and high levels of security awareness.

Organisation size and complexity should determine how regularly risks should be monitored and reviewed, but an annual review or risk management processes is recommended at a minimum.

**Outcome** – Continual monitoring of risks and update to treatment strategies where required.