



## Risk Assessment Advisory for Critical Infrastructure Data Storage or Processing 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 Data Storage or Processing 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 **Data Storage or Processing Sector** are outlined below:

**Key economic driver** – critical for other sectors and Australia's economic and social wellbeing. This sector will underpin many of the new technologies of industry 4.0.

**High downstream dependency** – provides services to all other sectors.

**Multinational critical infrastructure** – some providers are global, bringing together societal economies of scale and best-in-class services. This may create regulatory complexity for the organisation and its clients, given the range of competing national requirements and the offshore operating markets.

**High-value target** – for state actors, cyber criminals and hackers, given the ability to attack other critical infrastructure providers.

**Geographical and organisational complexity** – offshore data storage or processing presents both risks and opportunities for clients who operate or deliver services globally.

**High availability requirements** – any loss of availability in this sector may have a cascading effect on all other sectors.



## 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 Data Storage or Processing Sector is framing a possible risk from loss of power to a data centre caused by a natural hazard as to how it may disrupt the availability of a critical data storage or processing asset, as well as affecting the asset's critical downstream customers who have a dependence on the site for data storage or processing.

### 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 Data Storage or Processing Sector has been provided in the **Understanding sector-specific risks** section of this document.

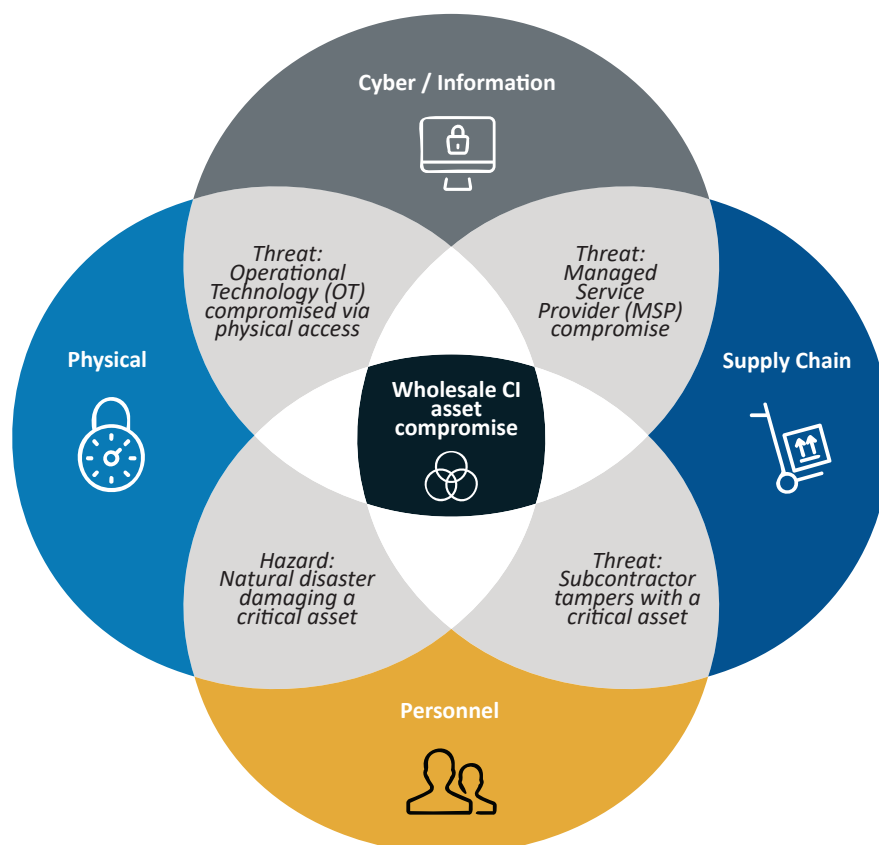
Some entities in the Data Storage or Processing Sector have security-related regulations already in place. Entities in the sector may need to consider guidance such as the Digital Transformation Agency’s Hosting Certification Framework, or look to their state or territory government for regulatory frameworks 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:*

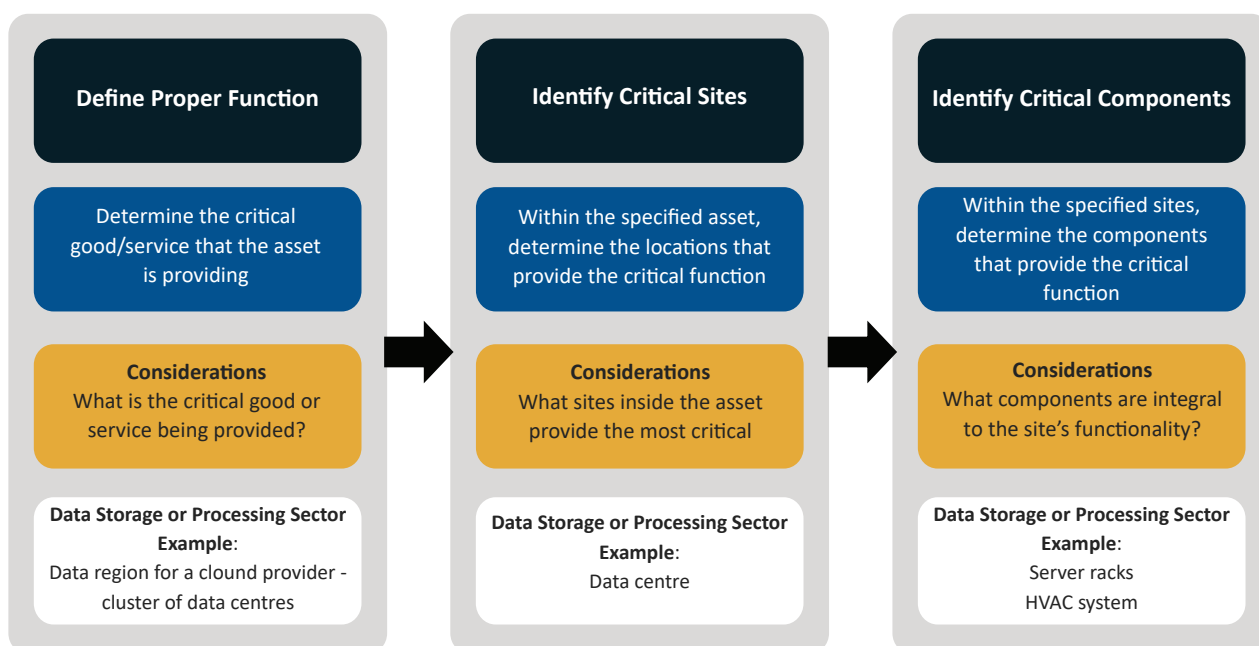
data storage or processing sector means the sector of the Australian economy that involves providing data storage or processing services

### Identifying and assessing criticality

For Data Storage or Processing 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 data centre in Canberra has been identified as critical due to its importance in providing data storage and processing capabilities to government, defence, and national critical infrastructure. The proper function of this asset may be defined as being able to deliver secure, sovereign and connected large-scale, multi-tenanted data centres to customers.

Critical sites are physical locations that are critical for an asset to achieve its proper function. This could include a data centre machine room, where the central processing unit is located, or other areas based on the context of the specific asset. It is important to identify whether 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 data storage or processing organisation, critical components may include air conditioning that maintains the operational temperature of the machinery, or water-level monitoring equipment.



## 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 Data Storage or Processing Sector:

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

### Emerging Trends

- **Increased self-sufficiency:** Data storage or processing 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.
- **Extend storage architecture to the public cloud:** As customers begin their journey to the cloud, we see traditional storage teams expanding their knowledge and contributions to application in the public cloud.
- **Edge driving new data requirements:** IT organisations have to produce new ways of protecting the data generated at the edge while keeping that data secure.
- **Cyber threats are impacting data storage:** The threat of a cyber attack is real and organisations must proactively protect their data and facilities. Data Storage and Processing entities provide services to multiple tenants so are often targeted as a means of entry.
- **Cloud-like elastic on-demand pricing for data storage systems:** Elastic on-demand fees only get charged after an organisation uses the storage capacity. The best way for data storage system vendors to compete with cloud vendors is to provide this same pricing serve on premises.
- **Prioritising sustainability:** Sustainability is a growing focus in almost every industry. Potential customers are not just focusing on typical considerations like speed and storage capacity, but also looking closely at the environmental impact of various data centre providers.

### Emerging Technology

- **Containerised applications need storage too:** Most organisations are developing cloud-native architecture based on containers, but are struggling to provide persistent storage to these ephemeral container environments.
- **Data storage performance supremacy:** The continued need for lower latencies will drive down application response times.
- **Improving management of unstructured data:** Unstructured data is anything not stored in a structured database format and is the most abundant in the modern data age. This includes images, audio and machine-generated information. Technology like AI is helping to manage this kind of data and provide better search queries and control capabilities to unstructured data.
- **Multicloud and hybrid cloud:** A growing number of organisations seek greater flexibility and choice as their workflows grow in scale and complexity. These organisations are increasingly seeking to leverage multi-platform, multicloud and hybrid cloud architectures.
- **Storage as a service model:** Organisations have begun to expect IT resources like data storage to be provided as a service, eliminating the added complexity of supplying and configuring their own hardware.



## 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/>



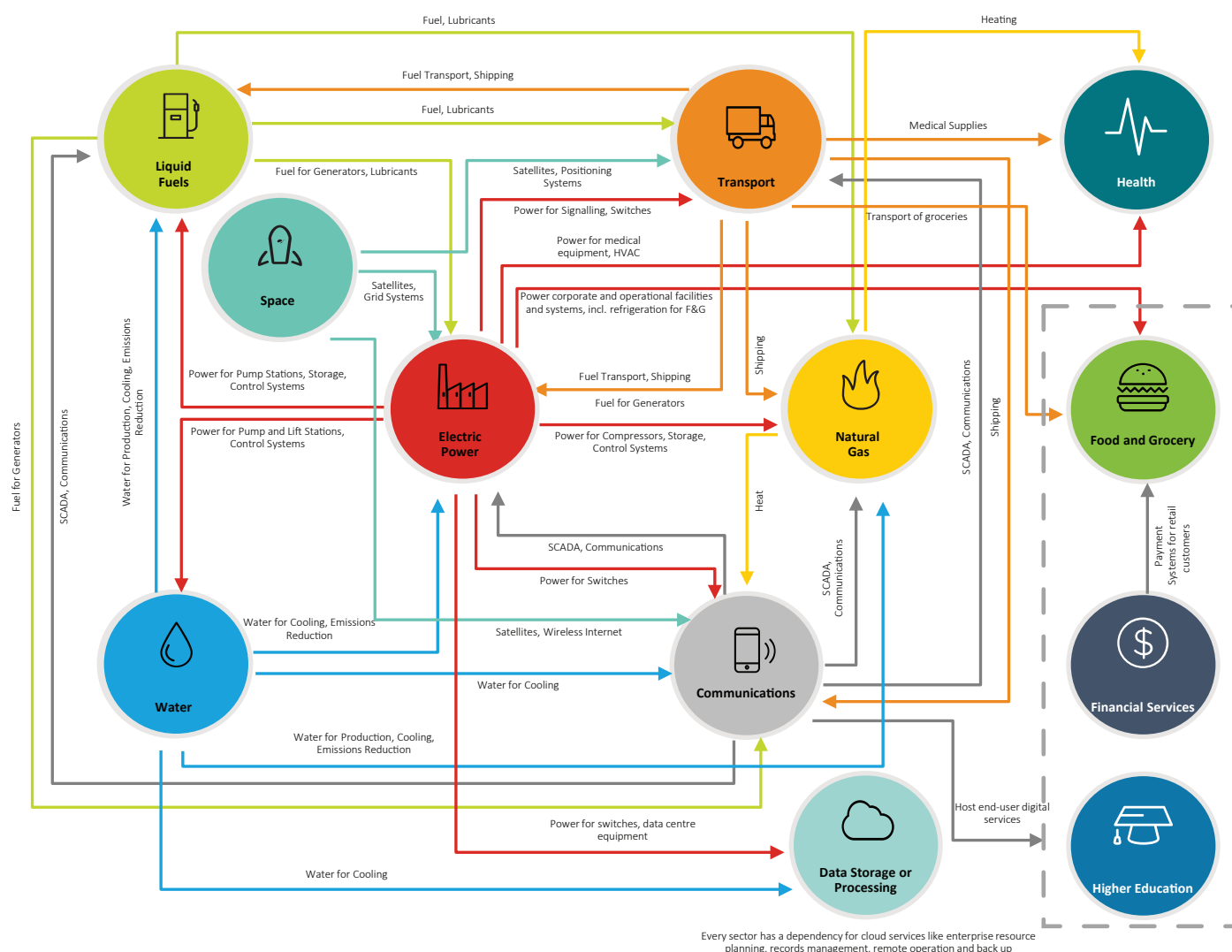
## Interdependencies (upstream and downstream)

### 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 Data Storage or Processing 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

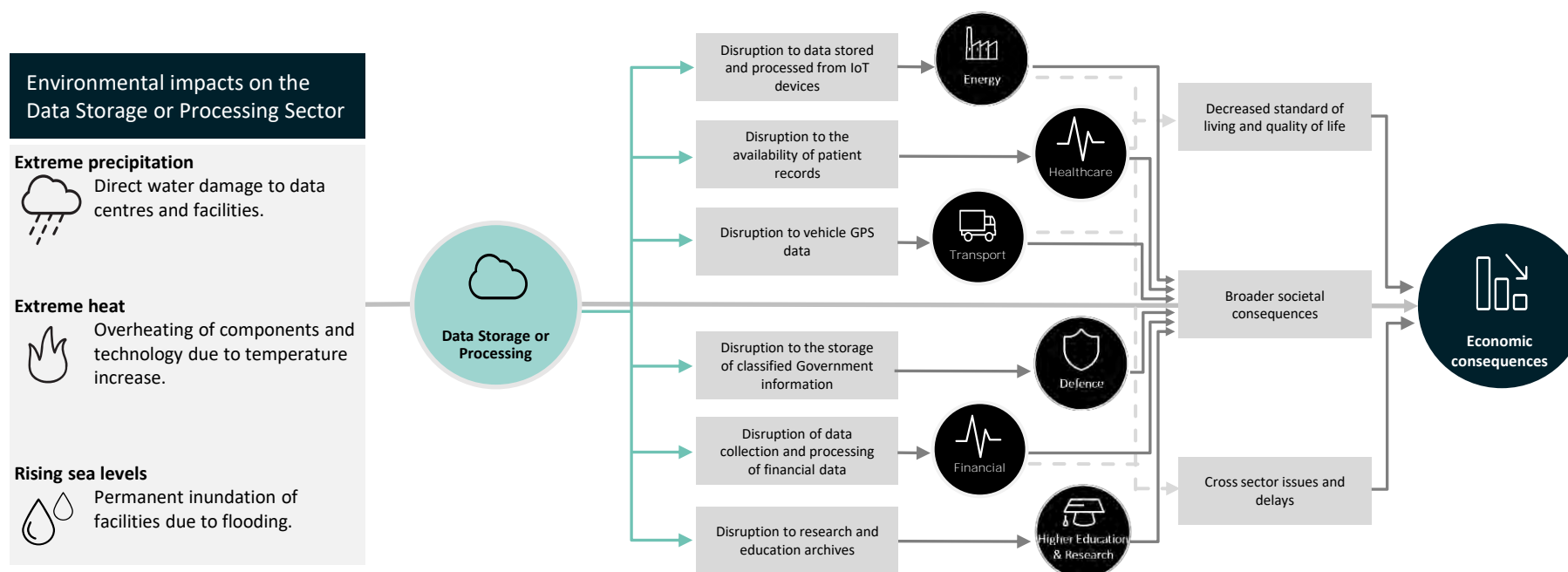




## Flow-on effects for relevant impacts against Data Storage or Processing Sector assets

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 Data Storage or Processing Sector.

Figure 5. Example of flow-on effects from an impact against the Data Storage or Processing Sector





An outage affecting a critical asset in the Data Storage or Processing Sector could result in significant economic or societal implications. Impacts could vary based on factors including the geographic breadth of the outage and the extent of impact on the broader data storage or processing network. For example:

- In 2022, a change to the network configuration at a large content delivery organisation led to an accidental outage, which caused major disruptions across the internet, affecting traffic in 19 data centres that handled a significant proportion of global traffic. No specific information about the extent of the disruptions was released, but some users may have been unable to access websites and services that relied on the organisation.
- In 2021, extreme heat in Perth and a malfunctioned cooling system caused a large data centre issue that resulted in email and web servers going offline. Businesses hosting their websites on the data centre's infrastructure were temporarily unable to access their sites.
- In 2021, a power outage at one of the data centres in a large data organisation in Virginia, USA brought down its services; there was a problem within the organisation at its US-East-1 cloud region that impacted customers and users of the data centre.
- In 2021, a company's Australia-Southeast-2 hosting region in Melbourne went down for 90 minutes due to transient voltage issues that rebooted network hardware, impacting all services that used the cloud network. In order to mitigate the issue, traffic within the region was temporarily redirected.
- Hurricane Sandy caused a sustained power outage which overwhelmed the backup power capability of many data centres in impacted areas following the storm. In a 2021 survey of data centre owners and operators, half the respondents indicated that the outage caused substantial financial, operational and reputation damage; furthermore, 69 percent reported experiencing some form of power outage over the past three years.

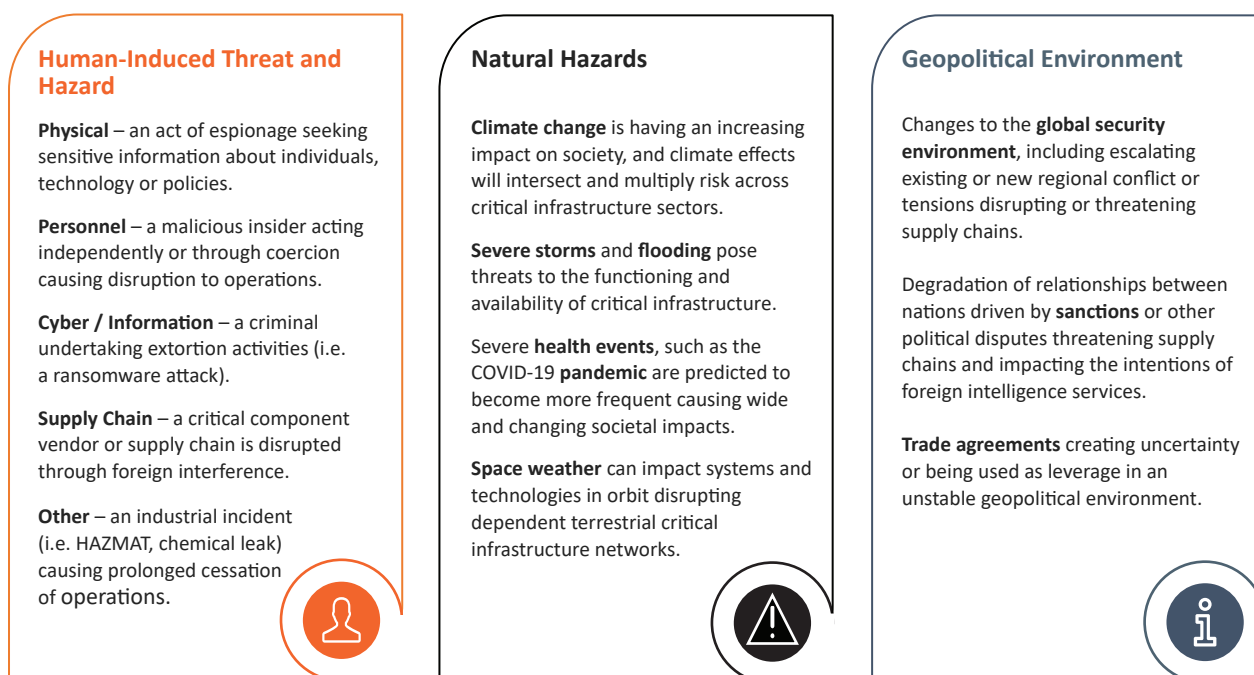


## Understanding threats and hazards for risk

### Identifying a threat and hazard landscape of the Data Storage or Processing Sector

All-hazards risk assessment considers both human-induced and natural threats and hazards. Given its role in critical infrastructure, the Data Storage or Processing Sector is an attractive target for threat actors seeking societal disruption, and its high reliance on power supply leaves it susceptible to severe weather event causing energy disruption. A strategic representation of the threat and hazard landscape to the sector could be represented 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, as the Data Storage or Processing Sector – driven by improvements in technology and the need to meet commercial outcomes – becomes more interconnected this means that stakeholders in the Data Storage or Processing Sector need to re-evaluate risks regularly.

Natural hazards are becoming more frequent and intense, their impacts long and complex. The Data Storage or Processing Sector is susceptible to such hazards through damage to facilities and componentry.






## Understanding sector-specific risks

This table outlines a select example of identified threat and hazard vectors that impact Data Storage or Processing 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 specific data centres 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 data storage and processing.
	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 storage or processing 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 data storage providers has the potential to halt the functioning of an asset for extended periods with the intent to extract financial benefits.
 NATURAL	Pandemic	<ul style="list-style-type: none"> <li>Availability</li> <li>Reliability</li> </ul>	Pandemics such as COVID-19 have the potential to greatly alter the functioning of society, with developments such as higher demand on corporations' remote-access data processing requirements.
	Severe weather events	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> <li>Reliability</li> </ul>	With increasing extreme weather events, data storage or processing infrastructure is likely to be impacted by more frequent extreme weather and natural disasters, causing damage to the output and functioning of the sector.

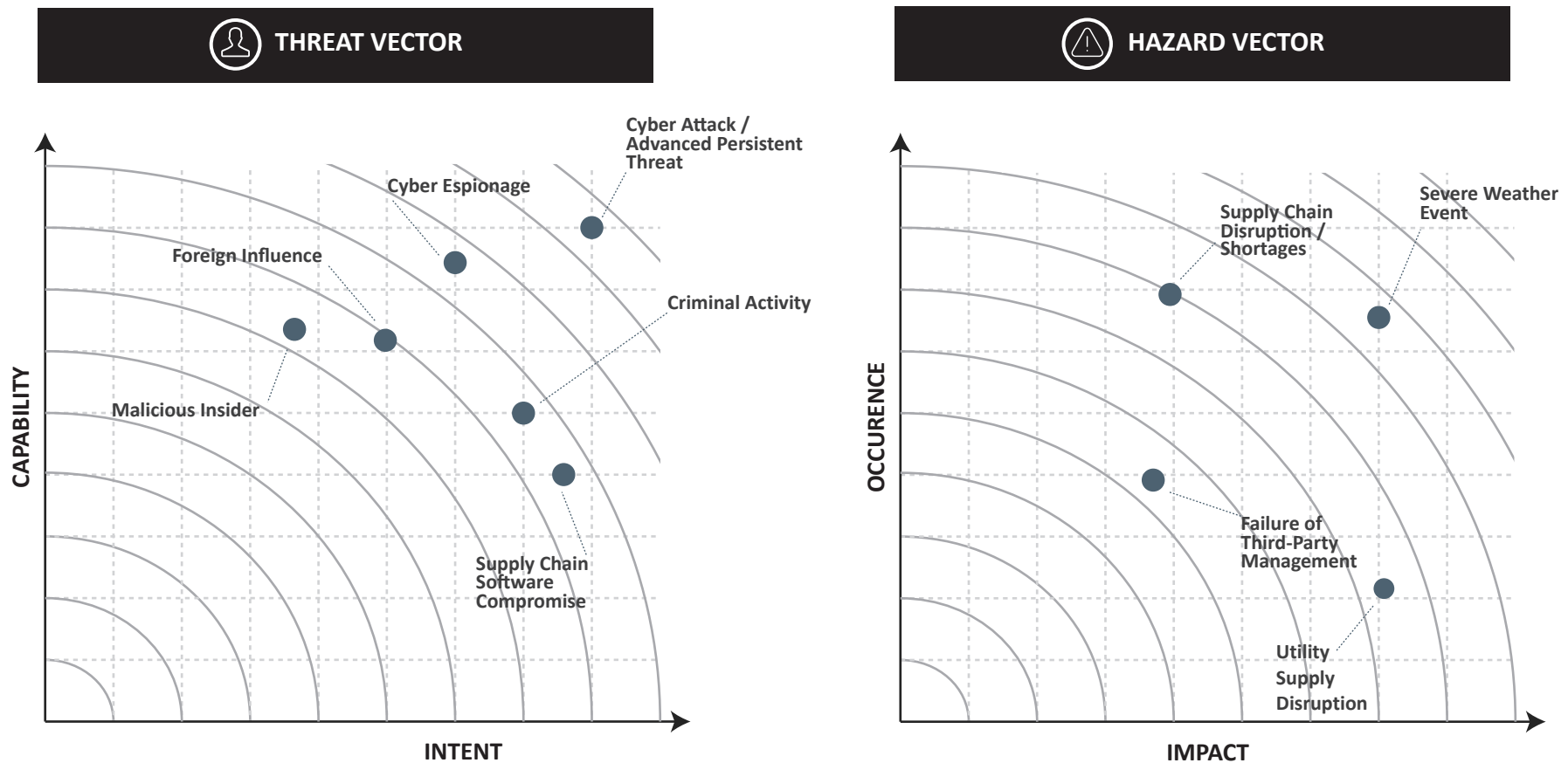


	Threat or Hazard Vector	Area of Potential Impact	Risk Scenario Considerations
 PHYSICAL	Foreign Interference	<ul style="list-style-type: none"><li>Confidentiality</li><li>Availability</li><li>Reliability</li></ul>	Foreign ownership in Australia's data centres may be subject to interference from foreign adversaries, using access or coercion to gain access to stored data.
	Criminal activity	<ul style="list-style-type: none"><li>Confidentiality</li><li>Availability</li><li>Reliability</li></ul>	Criminal activity can damage Data Storage or Processing Sector infrastructure; for example, via unauthorised access to a site with the intent to steal physical assets.
 SUPPLY CHAIN	Managed service provider compromise (supply chain compromise)	<ul style="list-style-type: none"><li>Confidentiality</li><li>Availability</li><li>Reliability</li></ul>	The sector relies on third-party resource providers, which have the potential to fail or become compromised, affecting downstream service providers in the sector.
	Supply issues/shortages	<ul style="list-style-type: none"><li>Availability</li><li>Integrity</li><li>Reliability</li></ul>	Data Storage or Processing Sector providers often rely on electronic components from overseas (i.e. semi-conductors). Issues in the supply chain, such as trade sanctions, conflict or supply shortages, may affect the availability of critical 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 through deliberately sabotaging data storage and/or processing through intimate knowledge of operations and possible clients.
	Utility supply disruption	<ul style="list-style-type: none"><li>Integrity</li><li>Availability</li><li>Reliability</li></ul>	Hazards, such as an accidental maintenance incident can cause significant risk for an entity. For data centres, an incident that causes disruption to the provision of power could have a significant impact.

## 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 Data Storage or Processing 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:

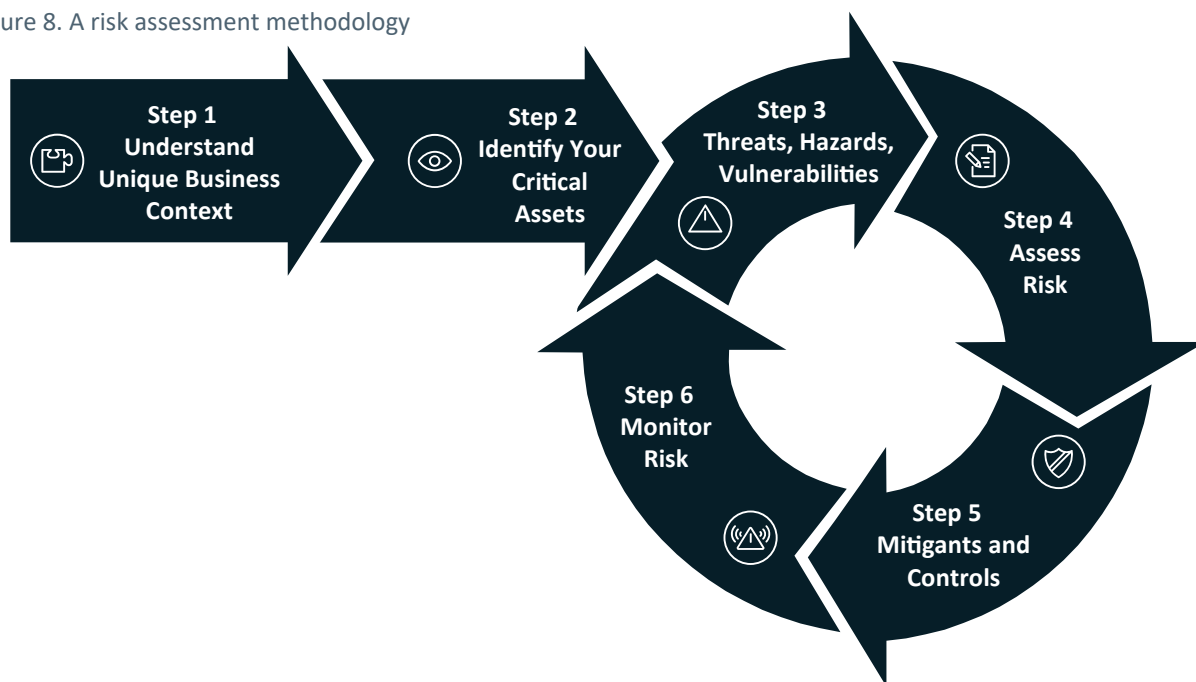
- Ease of implementation
- Cost-effectiveness
- Whether the action creates new risks and/or unintended consequences
- Environmental impacts (positive and negative)
- Multi-objective actions
- Long-term and short-term results
- Effectiveness
- Direct and indirect benefits
- Legal, regulatory, social and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



## Appendix – A risk assessment methodology

Data Storage or Processing 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 Data Storage or Processing 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.