



# Risk Advisory for Critical Infrastructure Data Storage or Processing Sector February 2026 (version 2.0)

This advisory has been designed to provide guidance to critical infrastructure owners and operators on assessing risks to Australia’s Data Storage or Processing Sector, and to complement the Critical Infrastructure Annual Risk Review. This risk advisory should also be read in conjunction with the risk advisory *Assessing risk for critical infrastructure*.

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 a widening array of threat actors. The Data Storage or Processing Sector (the Sector) is a vulnerable target in many ways. For example, even in a high security environment like that of data centres, malicious insiders have a level of access that could enable significant disruption. As a result, stakeholders within the 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.

Risk issues are presented under the hazard categories outlined in the *Security of Critical Infrastructure Act 2018* (SOCI Act) and accompanying *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* (CIRMP). This advisory considers the following topics:

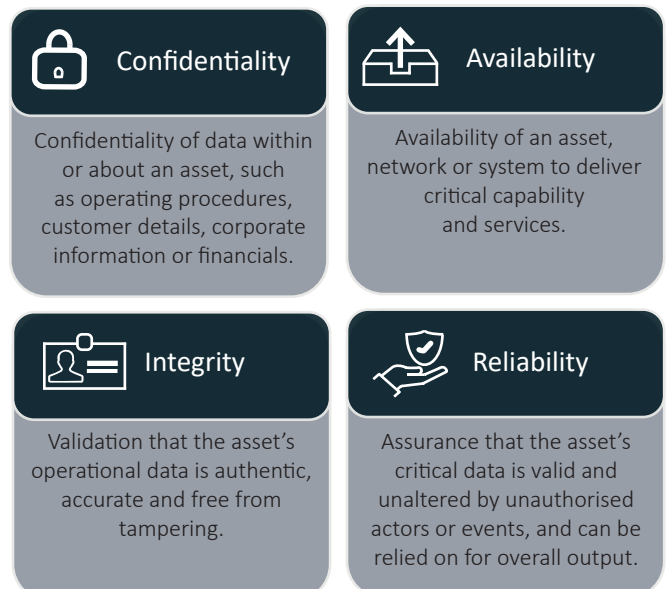
- Identifying and assessing relevant impact.
- Risk considerations by hazard category.
- Threat and hazard prioritisation.
- Sector interdependencies.

## Identifying and assessing impact

Understanding a potential ‘relevant impact’ is important to prioritising risk and determining how best to both minimise the likelihood of the risk occurring and mitigating the potential impact.

For example, an outage affecting a critical asset in the Sector could result in significant economic or societal implications. Impacts could vary based on factors including the geographic breadth of the outage, and the magnitude of the impact to the broader network. Impact can be assessed in several ways and should form part of a risk consequence assessment. When identifying a relevant impact on national critical infrastructure, entities should also consider an impact on the availability, integrity or reliability of a critical infrastructure asset, or the confidentiality of information about or within a critical infrastructure asset (Fig. 1).

Fig 1. Areas of relevant impact identified in SOCI Act.





## Cyber and Information

**Cyber and information** security hazards include where a person, whether authorised or not: (a) improperly accesses or misuses information or computer systems about or related to the critical infrastructure asset; or (b) uses a computer system to obtain unauthorised control of, or access to, the critical infrastructure asset that might impair its proper functioning.

Cyber and information security hazards to critical infrastructure pose new and innovative risks each day with increasing digitisation, the development of new technology, artificial intelligence (AI) capabilities, and increasing convergence of information technology (IT) and operational technology (OT). Malicious cyber actors may seek to extract critical information, compromise or sabotage systems or OT, or pre-position on networks for future disruption of critical functions.

Threat actors may use cyber means to gain unauthorised access to the Sector’s information for a range of purposes including theft, extortion or espionage. Emerging technologies, including AI, quantum computing, and machine learning, will increase the ability to rapidly de-encrypt huge datasets, conduct intellectual property (IP) theft, and generate strategic advantage through espionage of critical data, requiring data providers to continuously evolve their cyber security practices to pre-empt and address new threats.



### Cyber and Information risk considerations for Data Storage or Processing Sector

VECTOR	AREA OF IMPACT	EXAMPLE OF RISK
Cyber espionage	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Data storage or processing providers store and access enormous amounts of critical data. Cyber espionage could be used to exfiltrate, monitor, intercept and manipulate data pertaining to Australian citizens’ personal information, government data, sovereign research and development, or critical infrastructure operating systems.
Cyber sabotage	<ul style="list-style-type: none"> <li>Integrity</li> <li>Availability</li> </ul>	If harnessed effectively, cyberattacks can be used to inform cyber sabotage attacks, to gain control of OT, indefinitely suspend or otherwise degrade capability. Sabotage to data centres or data providers could significantly disrupt critical services employed by other critical infrastructure sectors.
Criminal activity	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Cyber criminals are likely to conduct opportunistic attacks that target data centres and processing facilities. Ransomware deployed into the networks of data storage or processing providers has the potential to halt the functioning of an asset for extended periods, and/or give opportunity for an adverse actor to threaten the release of sensitive information, with the intent to extract financial benefits, on behalf of state actors, or for political reasons.
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 threat entities or other modus operandi to scope, exert influence and/or disable specific data centres to create disruption or cessation of communication and data services. Providers who store or process government data, IP, or personal data are likely to be targeted by foreign adversaries.
Remote access	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Remote technology is often used to access interfaces between an asset’s IT and OT systems, meaning support to data processors and storage can be managed remotely. This can be exploited by malicious actors to gain quick and easy access to critical systems.



## Supply Chain

**Supply chain** hazards include malicious actions to exploit, misuse, access or disrupt the supply chain; an over-reliance on particular suppliers, and other disruption from issues in the supply chain, including a failure or lowered capacity of supply.

Supply chain hazards occur when a supply chain is interfered with or disrupted, potentially compromising the ability of critical infrastructure to deliver its critical services.

Disruptions to the Sector’s supply chain can also occur as a result of natural hazards, such as storms which may damage supply facilities.

The Sector relies on the global market to source hardware and software from international suppliers and services. For example, the Sector is heavily reliant on the global supply of semiconductor products.

Training and recruitment also form part of the supply chain, and the Sector is experiencing skills shortages, which is exacerbated by a lack of investment within the Sector.



### Supply Chain risk considerations for Data Storage or Processing Sector

VECTOR	AREA OF IMPACT	EXAMPLE OF RISK
Supply shortages	<ul style="list-style-type: none"> <li>Integrity</li> <li>Availability</li> <li>Reliability</li> </ul>	The Sector’s long global supply chains expose the Sector to a range of risks, such as trade-related risks, including piracy and sanctions; and business-related risks, including business failures, financial and other crime and concentrations in the supply chain. The supply of critical componentry for data centres or other assets can also be influenced by deteriorations in geopolitical relations, such as an increase in regional tensions or full cessation of supply from single source locations.
High risk vendors	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> <li>Reliability</li> </ul>	Suppliers to the Sector may be at risk of providing goods that have been sabotaged or manipulated to enable threat access to critical infrastructure.
Foreign ownership	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> <li>Reliability</li> </ul>	Foreign ownership of key links in supply chains may allow access to sensitive information. Parts sourced from overseas may also be subject to interference from foreign adversaries, which could include sabotaged or manipulated components that enable threat access to critical infrastructure in Australia.
Failure of third-party management	<ul style="list-style-type: none"> <li>Integrity</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.
Geopolitical tensions	<ul style="list-style-type: none"> <li>Integrity</li> <li>Availability</li> <li>Reliability</li> </ul>	The supply of critical componentry can be influenced by deteriorations in geopolitical relations, such as an increased in regional tensions or full cessation of supply from single source locations.
Interdependency disruption	<ul style="list-style-type: none"> <li>Integrity</li> <li>Availability</li> <li>Reliability</li> </ul>	The Sector is heavily reliant on a constant and reliable energy, communications and water supply for the assurance of operations.



## Physical

**Physical** security hazards include the unauthorised access to, interference with, or control of critical infrastructure assets, to compromise the proper function of the asset or cause significant damage to the asset.

Physical security hazards to critical infrastructure assets can manifest in a number of ways, through espionage, sabotage, and foreign interference. While physical security threats have historically been uncommon in Australia, the potential impact of operational disruption could be significant. Shifts in the global security landscape, including the escalation of regional conflicts or tensions, and the deterioration of international relations due to sanctions or political disputes over trade agreements, can increase physical security risks.

Such threats are often used as tools for geopolitical disruption. The Sector hosts data centres across Australia, primarily concentrated around Brisbane, Sydney, Melbourne, and Perth. Physical security across the Sector is of a generally high standard, however, threat actors may target supporting nodes or services, such as connectivity with other sectors, rather than the Sector’s data itself. Further, connectivity between multiple physical sites which operate as one may be targeted, causing disruption to sites’ services.



### Physical risk considerations for Data Storage or Processing Sector

VECTOR	AREA OF IMPACT	EXAMPLE OF RISK
Foreign interference	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> <li>Reliability</li> </ul>	Foreign ownership in Australia’s data networks presents risks, including the potential for a foreign government to compel a technology vendor or data provider to provide access to sensitive data sets, or undermine Australia’s national security interests.
Extremism	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Whilst unlikely given the physical security around data centres, threat actors may sabotage assets in the Sector, including through damage to data centres, cloud infrastructure and wider networks. Sabotage of dependent services that the Sector relies on, such as water services, may also disrupt the Sector’s services.



## Natural Hazard

**Natural Hazards** include damage or disruption from fire, flood, cyclone, storm, heatwave, earthquake, tsunami, space weather or biological health hazard (such as a pandemic).

Natural hazards can have severe consequences. The effects of climate change will continue to impact on society, and climate effects will intersect and multiply risk across critical infrastructure sectors. Detrimental health events, such as the COVID-19 pandemic are predicted to become more frequent, causing more widespread societal impacts. Space weather can impact systems and technologies in orbit, disrupting dependant terrestrial critical infrastructure networks.

The Sector is highly vulnerable to physical damage caused by natural hazards.

Severe climate events, such as excessive heat, can impact data centre cooling systems, which are required to manage the temperatures generated by data centre servers. Whilst shutdown of servers may not lead to loss of all data, it is possible that some servers may shutdown without replicating their current state, leading to loss of some unsaved data. Severe storms can also damage key enabling utilities, causing outages which can disrupt communications between data centres, and subsequently impact services provided to other critical infrastructure sectors.



### Natural Hazard risk considerations for Data Storage or Processing Sector

VECTOR	AREA OF IMPACT	EXAMPLE OF RISK
Severe weather event	<ul style="list-style-type: none"> <li>Integrity</li> <li>Availability</li> <li>Reliability</li> </ul>	More persistent, unpredictable and dangerous weather events and natural disasters may degrade the physical infrastructure supporting or storing data, causing critical data loss as storage or processing conditions become impacted. For example, flooding may impact data centres, which in combination with power outages, could restrict refuelling access.



## Personnel

**Personnel** security hazards include where a critical worker acts, through malice or negligence: (a) to compromise the proper function of the asset; or (b) to cause significant damage to the asset.

Personnel security hazards manifest through both intentional and unintentional vectors. Australia’s critical infrastructure is relatively robust to external, physical attacks, but mitigating and protecting against threats from within is more difficult, because insider threats already have the knowledge and legitimate access to damage systems significantly. Trusted insiders are one of the most attractive targets for external threat actors, as they can be recruited for malicious activity through monetary or ideological incentive.

Trusted insiders within the Sector can cause significant damage through the accidental or deliberate disclosure of privileged information, unintended or intended removal of local data, or manipulation of systems to allow third-party access. External threat actors could also take advantage of existing employees or pre-position people in roles with high-level access to data or network security and associated systems.



### Personnel risk considerations for Data Storage or Processing Sector

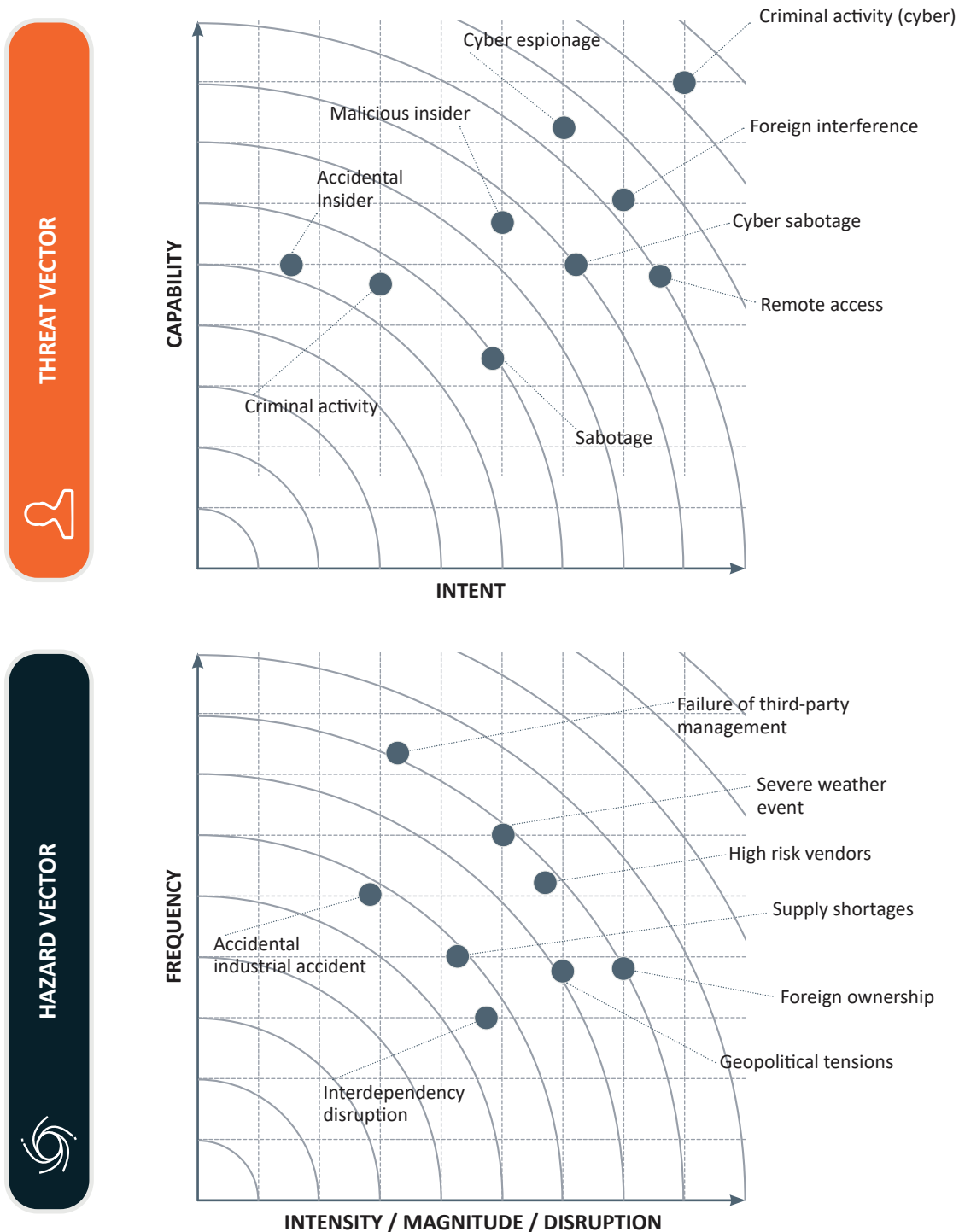
VECTOR	AREA OF IMPACT	EXAMPLE OF RISK
Negligent or accidental insider	<ul style="list-style-type: none"> <li>Integrity</li> <li>Availability</li> <li>Reliability</li> </ul>	Negligent or accidental insiders do not have ill intentions, but their carelessness can expose critical infrastructure to external threats. Within the Sector, employees with privileged access to facilities, systems and databases, as well as workers along the supply chain, pose a great risk if they are negligent. For data centres, an incident that causes disruption to the provision of power, or a negligent employee letting through a malicious actor, could have a significant impact.
Malicious insider	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> <li>Reliability</li> </ul>	Malicious insiders are those who have intent to cause disruption or destruction of critical infrastructure functions or services. Employees or contractors with knowledge on data centre IT and OT could pose a significant threat if they have malicious intent, but even support services such as construction, cleaning, security and maintenance personnel could provide access to share information about data centre locations, equipment and infrastructure.

### Threat and hazard prioritisation

Prioritisation of risks is a key process in developing risk management programs. Risk prioritisation enables improved resource allocation, enhanced decision-making, and a more proactive and efficient risk management approach. Resources available to risk managers can be limited, and risk prioritisation allows entities to break down risk into manageable pieces that are adapted into a desired risk management strategy.

The diagram below illustrates an approach to the prioritisation of threat and hazard vectors by mapping threats against intent and capability, and hazards against frequency and intensity/magnitude/disruption levels.

Fig 2. Illustrated example of threat and hazard prioritisation for risk assessment.



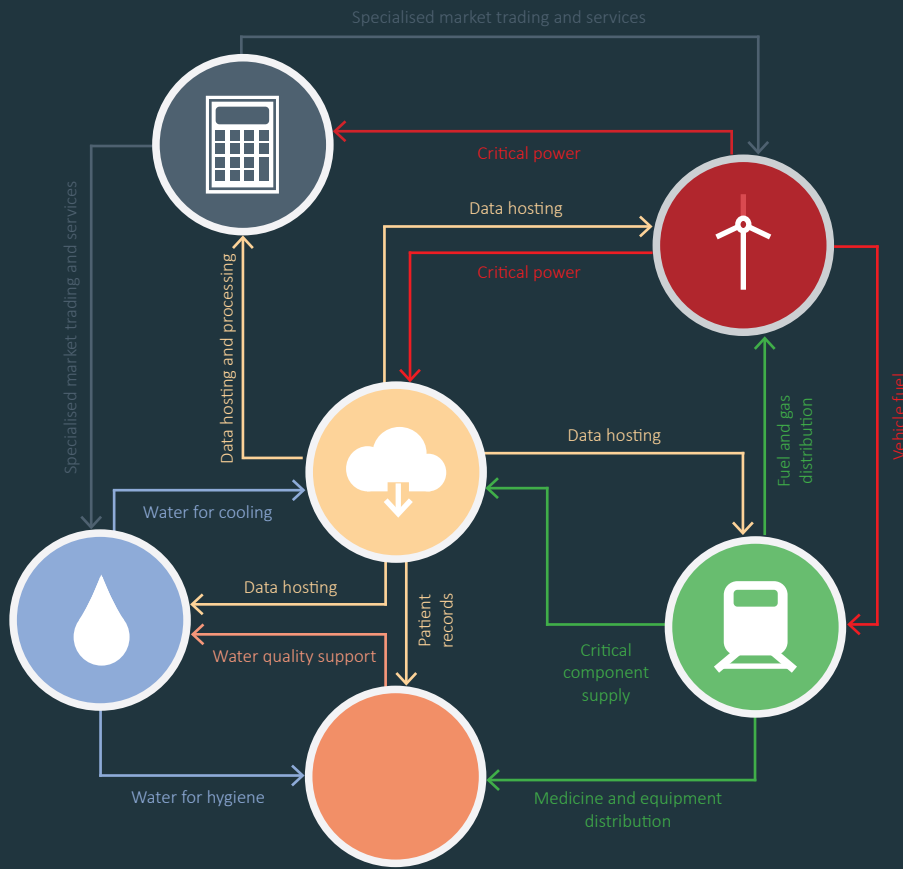


### Sector Interdependency

Australia's critical infrastructure sectors are deeply interconnected. Significant disruption in one sector will affect other sectors. Cascading effects from a significant incident to an entity in the Sector to other infrastructures should be distinguished and analysed as part of critical infrastructure risk assessment.

The Sector is an upstream dependency of other critical infrastructure sectors as much as other sectors rely on its downstream services, as illustrated in the diagram below.

Fig 3. Illustrated example of sector interdependencies for the Sector.





### Where can I find out more?

Within the Department of Home Affairs, the Critical Infrastructure Security Centre (CISC) drives an all-hazards critical infrastructure risk management regime in partnership with government, industry and the broader community. The CISC assists critical infrastructure owners and operators to understand the risk environment and meet their regulatory obligations. More information can be found on the [CISC website](#) or by contacting [enquiries@CISC.gov.au](mailto:enquiries@CISC.gov.au).

Responsible entities of critical infrastructure are eligible to use AusCheck's [critical infrastructure background checking scheme](#) as a control to mitigate the risk of malicious trusted insiders

The Australian Signals Directorate (ASD) provides a range of advice at [cyber.gov.au](http://cyber.gov.au) to improve cyber security.