Australian Government
Department of Home Affairs

CRITICAL INFRASTRUCTURE SECURITY CENTRE

Risk Advisory for Critical Infrastructure

Assessing risk for critical infrastructure

February 2026

This advisory has been designed to provide guidance to critical infrastructure owners and operators on assessing risks for Australia's critical infrastructure, and to compliment the Critical Infrastructure Annual Risk Review.

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 state sponsored and criminal actors.

Critical infrastructure owners and operators should adapt their risk management strategies to ensure that risks to the operation of assets which are critical to the nation's economic and social wellbeing are being appropriately captured. The following topics are explored in this advisory:

- **Risk in the critical infrastructure context**. Contextual information focuses on 'problem identification' in order to identify the areas of risk that should be investigated.
- **Determining asset criticality**. A vital process in risk assessment, providing a key input into the identification and assessment of plausible risk events.
- **Cascading, compounding and converging effects**. Information on how to identify and assess sector interdependencies and their wider impacts for risk assessment.
- **Adopting an all-hazards approach**. Guidance for building all-hazards risk assessment into existing risk management processes.
- **Steps for effective risk mitigation**. A suggested approach for implementing effective risk mitigation.

Risk in the critical infrastructure context

Risk in the context of critical infrastructure is related to Australia's national security and socio-economic 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 impact the social or economic stability of Australia or its people, or that have the potential to undermine Australia's national security and resilience, need to be considered in critical infrastructure providers' existing risk management strategies.

Some critical infrastructure entities have security-related regulations already in place. Entities may need to consider sector-specific *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023* (CIRMP) guidance 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.

However, proactively framing risk in a national security context (within existing risk management strategies) will help efforts to improve Australia's national security and socio-economic resilience.

For additional information, read the CIRMP guidance on the CISC website.

Determining asset criticality

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.

Identifying asset criticality

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 the interest of Australia's national security and socio-economic resilience. Establishing criticality helps guide the effective allocation of resources to ensure the asset's operational capability is protected.

Proper function of a critical infrastructure asset refers to its role in providing essential goods or services that support the nation's economic or social wellbeing, defence, or security.

Critical sites are physical locations that are critical for an asset to achieve its proper function. This could include pump stations, chemical storage buildings, 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 understand its 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, those required to maintain the function of the asset, or those that could cause significant damage to the asset where they have been compromised, are missing or damaged.

Assessing asset criticality

Assessing criticality involves analysing how each of the identified critical assets may be exposed to, or harmed by, threats and hazards. This process is vital for risk assessment, providing a key input into the identification and assessment of plausible risk scenarios and events.

One approach to assessing levels of criticality is through an analysis and rating of how each of the identified critical assets contributes to the provision of services by considering the following elements of an asset disruption.

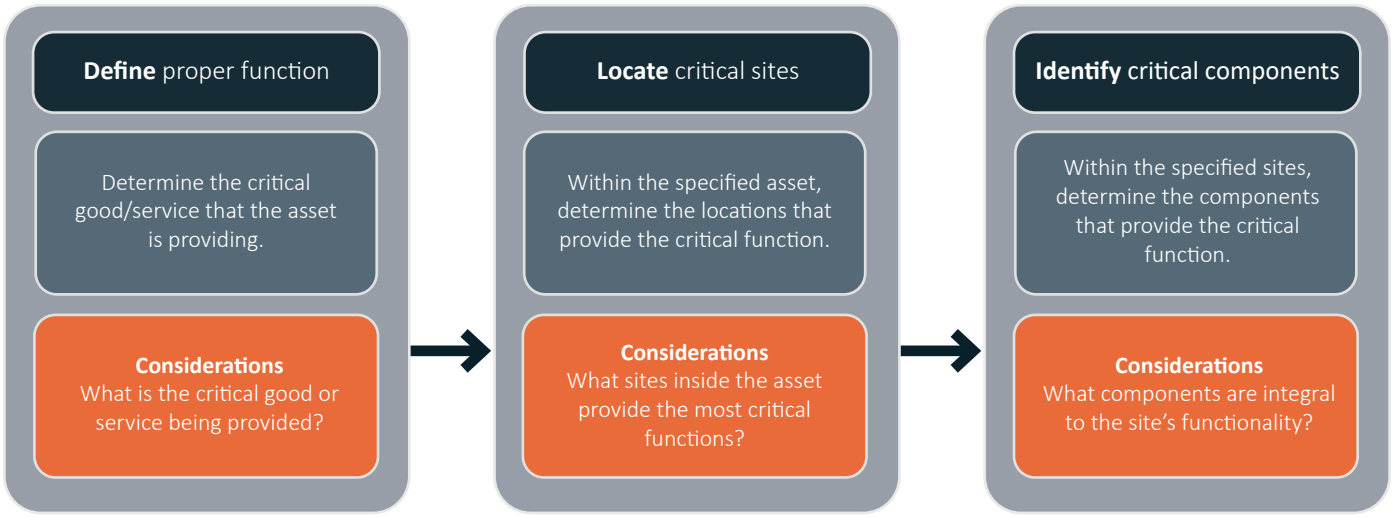
DEPENDENCY on the critical service by other critical infrastructure sectors.

How easy it is to **RECOUP** a critical service if its capabilities are disrupted or otherwise degraded.

The **TIME** it would take to return a critical service to its operational capacity

Each of these elements can be assessed individually to form a rating of criticality that is expressed as a combined consideration of criticality if a critical asset is no longer available.

Fig 1. An example of an approach for determining criticality.



Cascading, compounding and converging effects

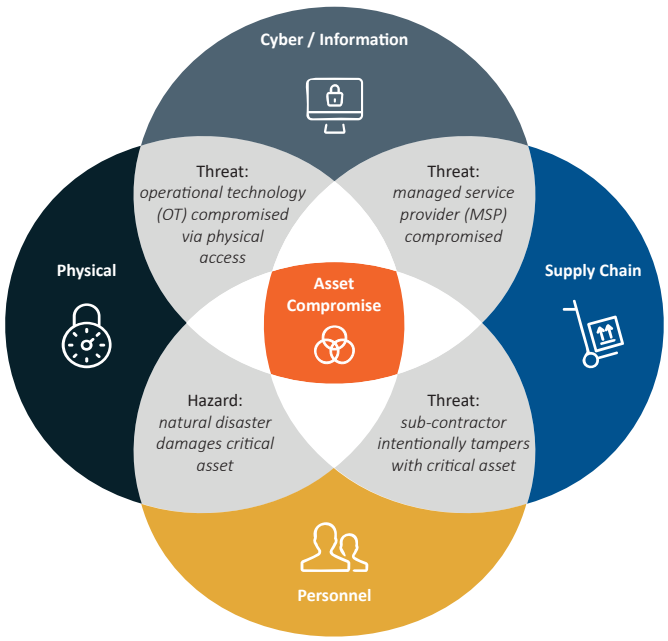
While it is difficult to predict the behaviour of an entire system simply based on the behaviour of one of the components, relationship analysis can help understand possible impacts from cause and effect.

A cascading effect can be nonlinear, where causal loop diagrams can be used to analyse linkages and 'cause and effect' relationships. Cascading effects can therefore increase the impact well beyond the original temporal and spatial components.

A compounding effect is one where the hazard can trigger follow-on sequences of other events that occur as a direct or indirect result of the initial triggering event. For example, power outages could be accompanied by communication failures and/or satellite malfunctions. These in turn could impact on telecommunications, positioning and timing, banking and finance, and transportation. In some cases, the problem would correct itself, for instance, radio or positioning, navigation and timing (PNT) links could come back online quickly, depending on the damage to infrastructure. In other cases, the impact may be longer lasting, where a burn-out electrical substation transformer takes weeks, months or even years to repair or be fully replaced.

Australia's adversaries pose an increasingly sophisticated threat to our critical infrastructure and often look to exploit multiple vulnerabilities via multiple vectors in unison.

Fig 2. Illustrated example of converging threats and hazards as part of risk identification.



Sector-wide convergence effects eventuate due to interdependencies within and across critical infrastructure sectors, as well as through other links, such as supply chain relationships (Fig. 2). Furthermore, convergence risks could exist within organisations due in part to internal silos or lack of integration of risk management capabilities.

Adopting an all-hazards approach

For critical infrastructure owners and operators, an all-hazards approach to determining risk is a requirement under the CIRMP. 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.

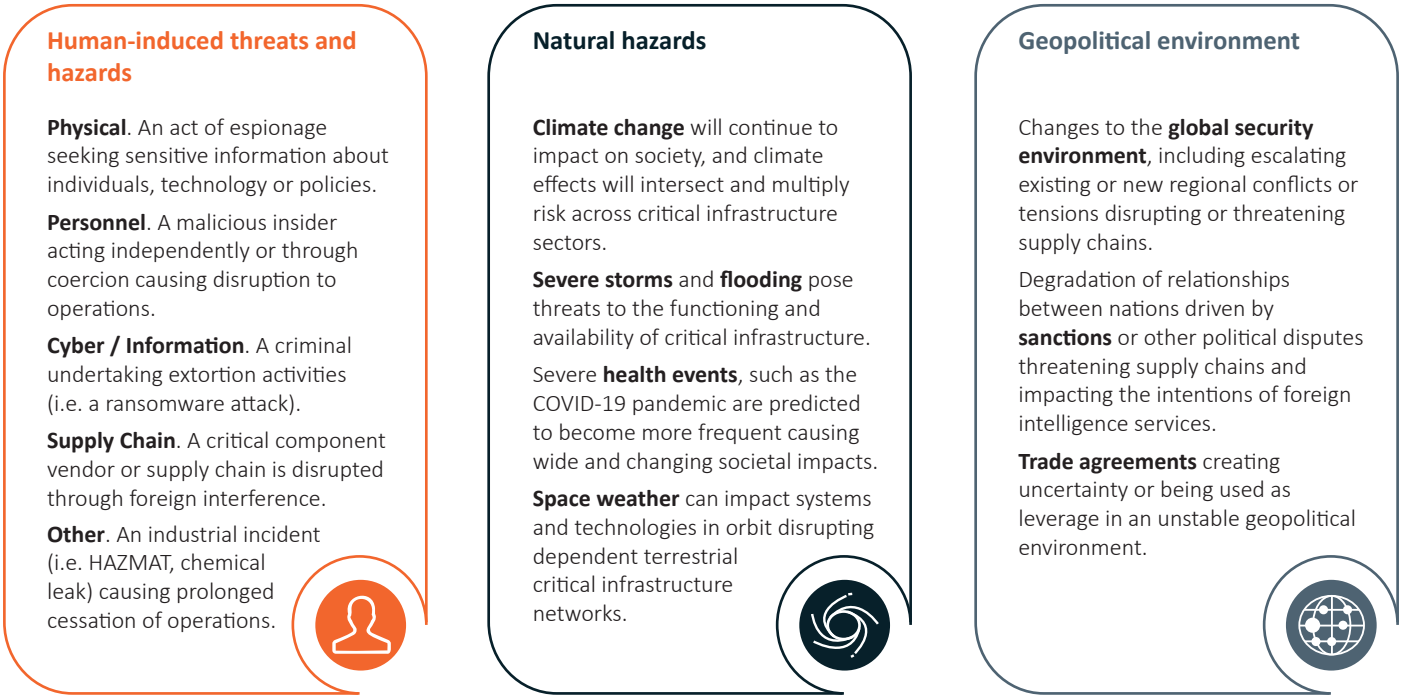
All-hazards risk assessment considers both threats (human-initiated) and natural and environmental hazards that could impact on a critical infrastructure entity and their operations. As Australia's critical infrastructure risk environment continues to evolve, an all-hazard risk approach is best placed to consider the potential convergence of the wide-ranging threats and natural hazards that could result in competing and cascading effects on national resilience.

Threat, hazard and vulnerability

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 category threats to critical infrastructure 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, as critical infrastructure – driven by improvements in technology and the need to meet commercial outcomes – becomes more interconnected. This means that stakeholders need to re-evaluate risks regularly. Natural hazards are becoming more frequent and intense, while recovery from their impact is longer and more complex.

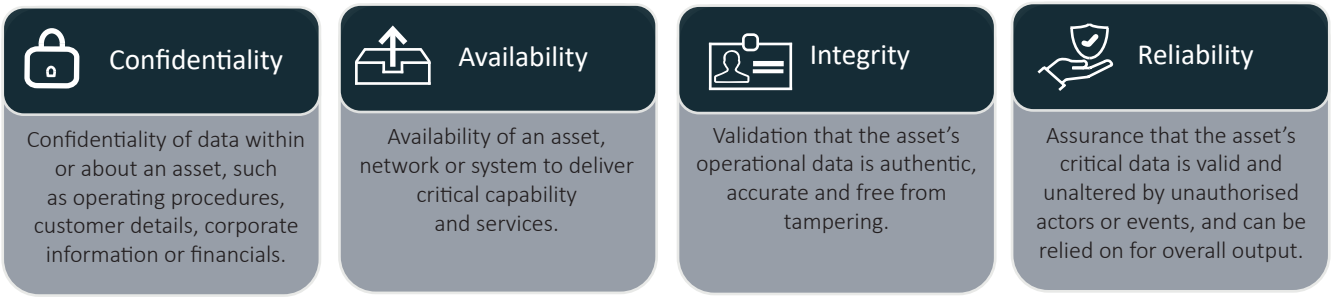
Fig 3. A representation of an all hazards landscape for critical infrastructure.



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 mitigate the potential impact. Impact can be assessed in several ways and forms 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. Understanding potential 'relevant impacts' is important so that the response to individual risks can be prioritised to gain the greatest return on investment in mitigation.

Fig 4. Areas of relevant impact identified in SOCI Act.



Four steps for effective risk mitigation

Risks may be poorly addressed at times, often because their causes or effects are misunderstood when identifying the risks themselves, or there is a lack of internal organisational guidance on how to effectively 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. Cross sector interdependencies may require a collective management approach to risk or may be too large for any single entity to address by itself. The following is a suggested four step strategic approach for implementing effective risk mitigation for critical infrastructure.

IDENTIFY all hazard risks to your asset/s.

Adopting an all-hazards risk management approach is a requirement under the CIRMP to ensure a comprehensive and integrated risk identification. This requires collaboration between a broader range of stakeholders (i.e. internal business units, sector and supply chain stakeholders, law enforcement and emergency services) to widen perspectives on how risk is addressed.

KNOW your drivers for impact management.

Organisations will have varying drivers that influence how risk impacts are managed and how mitigation strategies will be developed and prioritised. Knowing the key drivers for managing risk impacts goes beyond just an understanding of the organisation's risk tolerance and risk control funding. For example, should the focus be on mitigating against the most damaging impact or the most likely risk to impact; should vulnerabilities to external factors be targeted, or should internal issues be given a greater priority.

PRIORITISE risk treatment implementation.

Once controls and mitigation options have been identified, these should be continually evaluated and prioritised, particularly as threats and hazards evolve. The following criteria (right) can be used as a strategic guide for developing a prioritised approach for implementation of risk controls and mitigations.

- Ease and efficiency of implementation (time and duration).
- Cost-effectiveness.
- Immediate direct and indirect benefits.
- Legal, regulatory, social and moral obligations.
- Environmental impacts (positive and negative).
- Organisational equity and acceptability.
- Whether the action creates new risks or unintended consequences.

SHARE your risk outcomes.

Organisations can 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 Australian Government's national intelligence community also collects and analyses information to constantly monitor, assess and provide advice on threats to Australia. Part of their mandate include providing portals that host open-source information, assessments and advice designed to support critical infrastructure providers.

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.

Responsible entities of critical assets 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 to improve cyber security.