



Risk Assessment Advisory for Critical Infrastructure Transport 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 Transport 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 **Transport Sector** are outlined below:

Reliance on third parties

– including domestic and international collaboration, distribution centres and independent contractors.

Safety is at the centre of risk

– where the prevention of injury and loss of life is built into the fabric of the sector.

A large dependence on skilled labour

forces – as many workers have safety-critical operational responsibilities.

Collaboration with external entities

– which is required to maintain domestic international supply chains for both imports and exports.

Push towards lower/zero emissions – an area which is reactive to politics and policy.

Highly susceptible to physical threats – though acts of unlawful or operational interference.

Area of major public investment and economic importance – to maintain and expand transportation infrastructure as the Australia population grows.

Long-term infrastructure – much of which is designed to last for decades, and may not always be ready to be networked.

Heavy reliance on communications – all areas of transportation – air, land, and sea networks – are heavily reliant on the availability and integrity of communications and navigation information.

Susceptible to cyber attacks launched through third-party resource providers – cyber attacks are an increasing threat as assets are networked and reliant on operational technology.

The information contained in this document is general in nature and does not constitute legal advice. Readers are encouraged to obtain legal advice that applies to their particular circumstances. The Commonwealth of Australia does not guarantee the accuracy, currency or completeness of any information in this document.



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 Transport Sector is framing a possible risk from an act of physical damage to an intermodal transfer facility, whether from extremism or authorised access, as to how it may compromise the ability of the facility to operate, as well as the impact of critical downstream customers who have a dependence on the site to deliver goods currently stored.

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 Transport Sector has been provided in the **Understanding sector-specific risks** section of this document.

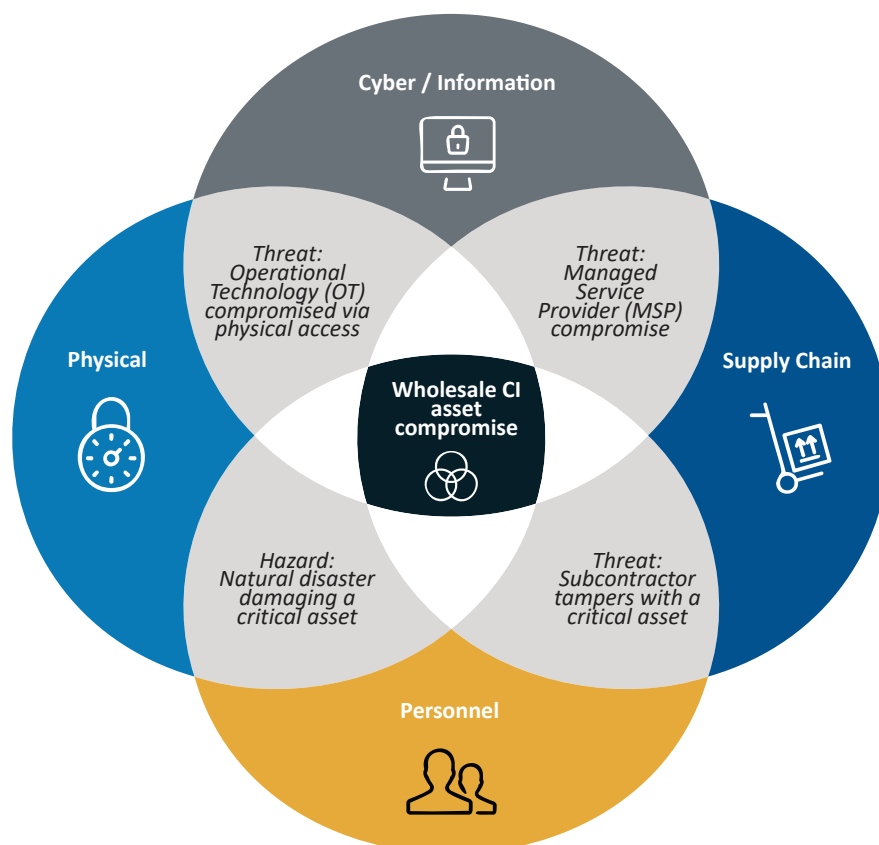
Some entities in the Transport Sector have security-related regulations already in place. Entities in the sector may need to consider guidance such as the Aviation Transport Security Act 2004 (ATSA), the Maritime Transport and Offshore Facilities Security Act 2003 (MTOFSA), or look to their state or 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:

transport sector means the sector of the Australian economy that involves:

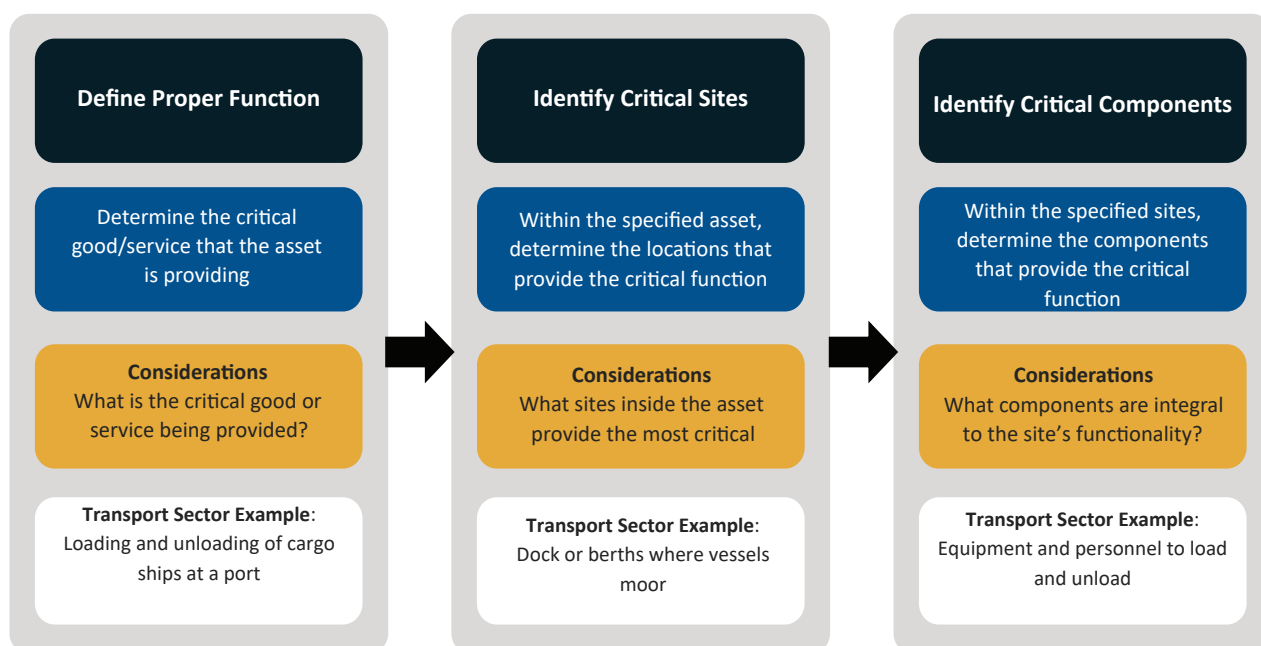
- (a) owning or operating assets that are used in connection with the transport of goods or passengers on a commercial basis; or
- (b) the transport of goods or passengers on a commercial basis.

Identifying and assessing criticality

For Transport 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.

Critical sites are those in which assets assigned proper functions are located. This could involve locations such as control rooms, loading bays, security operations centres, 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 should 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, compromise or damage could cause significant harm to the asset. For a transportation organisation, critical components may include enterprise resource planning (ERP) systems or port loading and unloading machinery.



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 Transport Sector:

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

Emerging Trends

- **Machinery as a service (MaaS):** The new form of transport giants such as Uber and Lyft have shifted parts of the sector to a less rigid 'transportation on demand' industry.
- **Diversification in methods of private transport:** From personal aircraft to electricity or hydrogen-powered vehicles, to autonomous vehicles, new developments present imminent, potentially disruptive forces in personal transportation. High-speed rail offers an alternative to flying for transportation between major hubs. Drones and automated transportation have the potential to revolutionise the ways logistics and distribution operates.
- **Climate change will continue to weigh on consumer minds:** Increased scrutiny from regulatory bodies will impact on Transport Sector providers to consider both current emissions production and the technologies that may be required to reduce it. While new technologies and more efficient processes reflect efforts to reduce the environmental impact of the sector, governments across the world are moving towards more ecologically sustainable policy standpoints and regulation.
- **Green public transportation:** This has increased across the states with widespread public support. These forms of transportation are usually offset or electric
- **Bicycles and human-powered transport:** These modes of transport have gained support in metropolitan areas where conventional methods are impractical. This is supported through advances in lithium batteries, allowing e-bikes to travel further than the have before.

Emerging Technology

- **High-speed rail networks:** Public support is increasing and the implementation of high-speed rail may decrease the use of private transportation in populated areas, driving growth in regional areas.
- **Operational Technology (OT):** This has expanded the Transport Sector's digital footprint presenting a risk in areas where assets are designed for long-term use, or in areas where there has been under-investment in security of infrastructure. OT systems are no longer isolated and therefore a cyber attack on an internet-connected OT system, or an attack that starts in the corporate environment and crossed into the OT environment, can have direct physical consequences.
- **Data analytics:** Increased methods of capturing data means that analytics can improve the overall efficiency of transport systems, coalescing through improved inventory management, use of resources and operational costs. Data analytics can help streamline processes when it comes to both online and offline channels.
- **Automation and robotics:** In recent years, decrease costs and requirements for employees in the workforce has led to efficiencies in the transportation of goods and warehousing.



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>



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/>



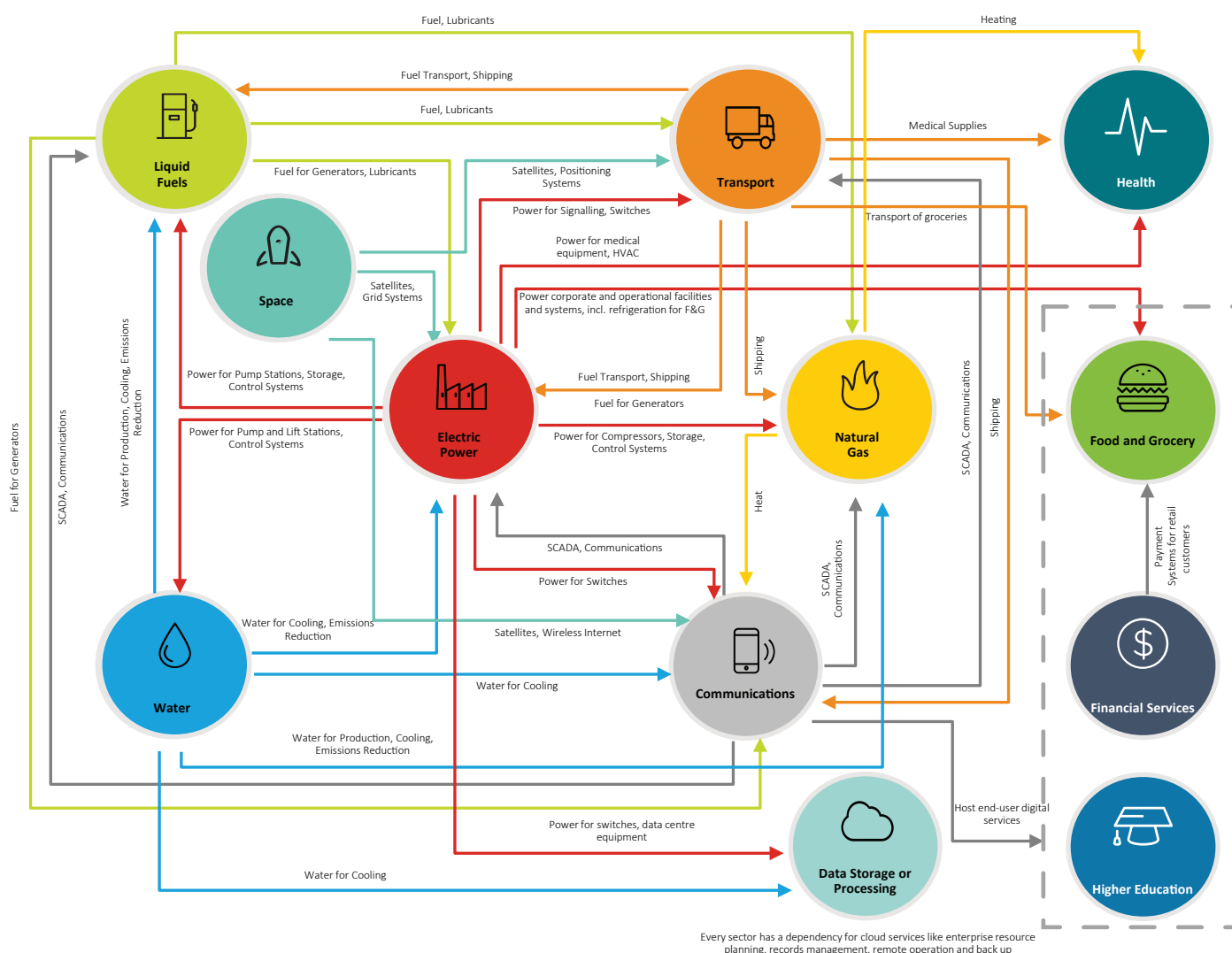
Interdependencies (upstream and downstream)

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 Transport 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

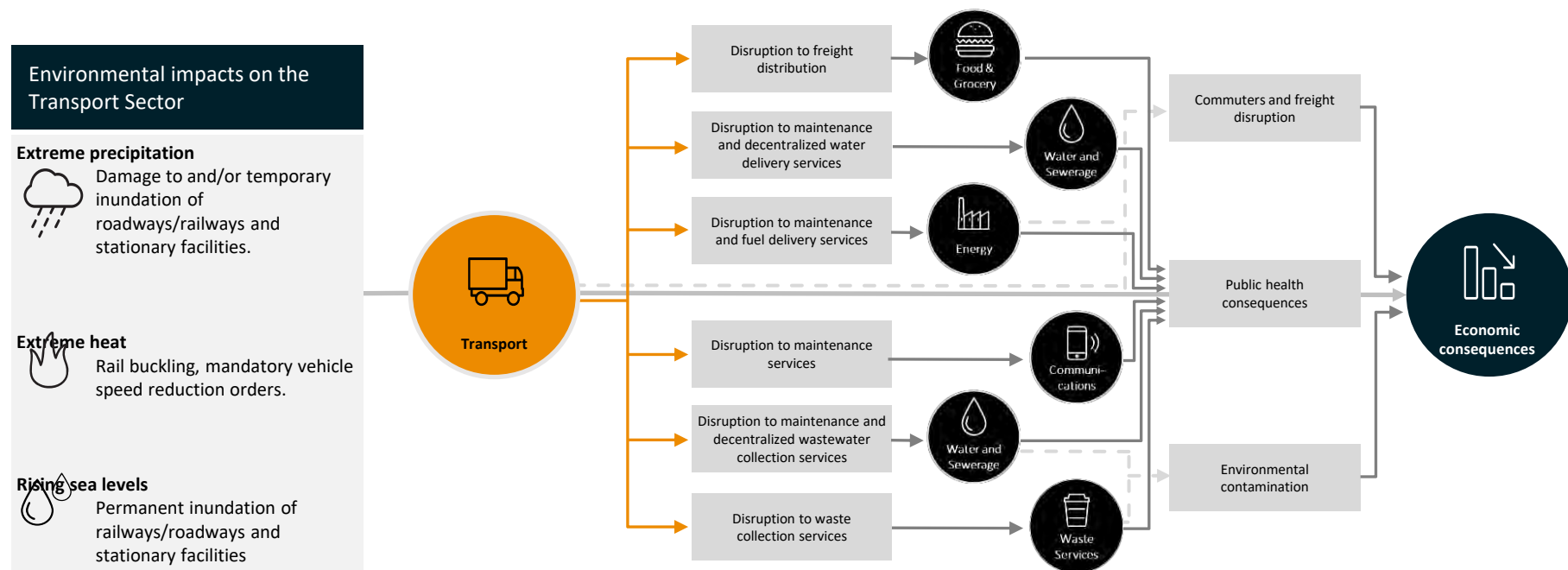




Flow-on effects for relevant impacts against Transport Sector assets

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 Transport Sector.

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





A disruption within the Transport Sector could have major downstream impacts on other critical infrastructure sectors and the Australian economy. This could range from lengthy worker commutes, halts on domestic and international travel, or delays to the transportation of goods that are necessary for other sectors to function. For example, entities in the Healthcare and Medical Sector may rely on perishable supplies, without which human life could be threatened, to be delivered regularly.

Downstream, the Australian economy and way of life is dependent on many international and domestic trade routes. All critical sectors depend on the Transport Sector for fuel, operational necessities, components for maintenance or medical supplies, and the transportation of personnel. Any disruptions to the Transport Sector can have widespread impacts on all critical sectors, the Australian economy and the public's safety and wellbeing.

Upstream, the Transport Sector is heavily dependent on the Energy Sector and the Communications Sector. Aviation and supply chains are heavily reliant on the Communications Sector to maintain operational connectivity, and on the Energy Sector to maintain fuel supplies and power infrastructure.

A major unplanned outage to a transport asset, system and/or network is likely to have substantial economic and/or societal implications, dependant on the asset, system, or network affected. The severity of an incident could be heightened depending on the geographic breadth of the outage, the services dependent on transportation, and the extent of the impact to Australia's broader logistics network. For example:

- In 2020, a large logistics company was hit twice by ransomware attacks that encrypted computer systems and demanded a ransom payment to unlock the files. The attack forced it to shut down a number of systems across multiple sites and business units, and led some customers to sign temporary agreements with competitors to maintain their own supply chain. These events highlighted the challenge an attack on a major logistics organisation can present to an entire supply chain.
- In 2017, a multinational logistics and transport company was a victim of a global release of NotPetya malware, a form of ransomware that encrypts all information it has access to. The corruption within the entity's systems effectively shut down for almost a week the global operations of the company, which operates 76 ports and is responsible for almost a fifth of global shipping operations; damages and recovery costs were estimated at USD250–300m.
- In 2016, an Australian public transport entity was forced to take its website offline during an attempted hack.
- Unavailability of aircraft, airline booking systems, and other networks within aviation organisations occur regularly, each time resulting in lost revenue or disruption to flights and delays in boarding times. This may occur through an outage of flight information systems or outages in booking and ticketing systems. Many airlines also leverage third-party services for operations and maintenance, as well as baggage and distribution systems, so an outage has the potential to cause major localised disruptions to the industry.
- The rail industry is becoming increasingly reliant on electronic sensors and networks, which have the potential to be interfered with or disrupted. Potential impacts can range from inaccuracies in positioning information, changes to switching infrastructure through sending of unauthorised signals (such as infra-red signals), or inaccurate telemetry from operating vehicles.

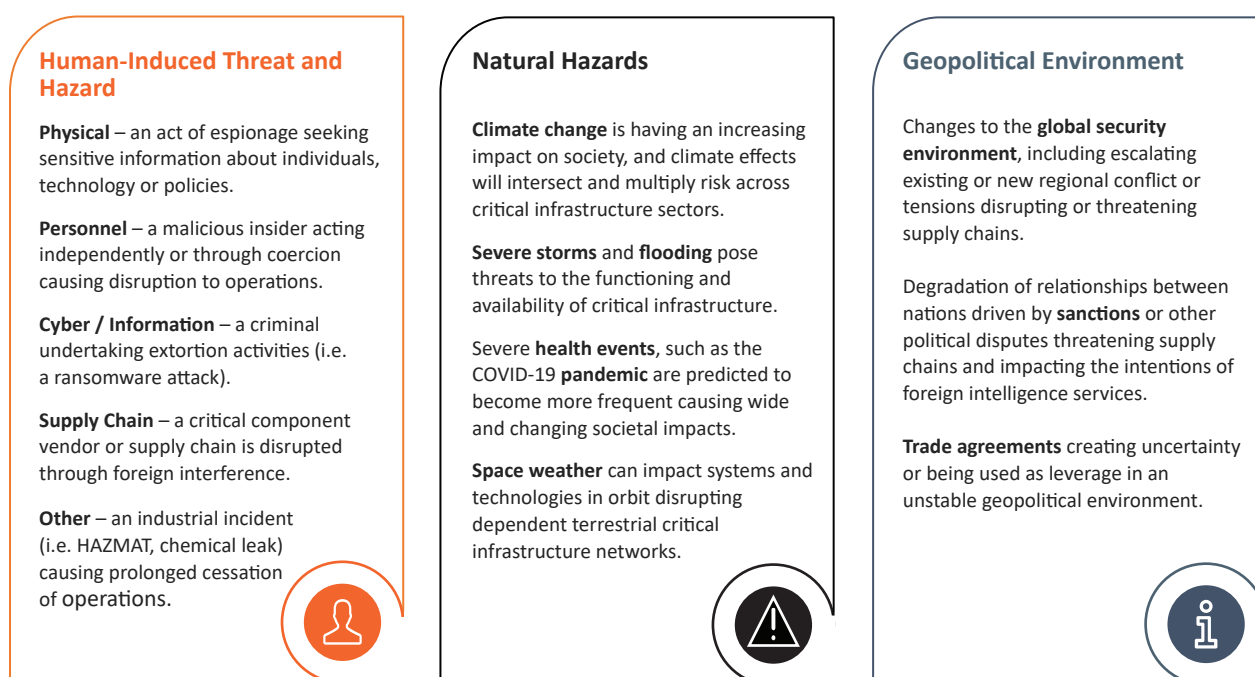


Understanding threats and hazards for risk

Identifying a threat and hazard landscape of the Transport Sector

All-hazards risk assessment considers both human-induced and natural threats and hazards. Given its significant role in critical infrastructure, as well as the key economic importance of its services; the Transport Sector is an attractive target for multiple types of threat actors, 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 Transport Sector, driven by improvements in technology and the need to meet commercial outcomes, will become more interconnected. This means that stakeholders in the Transport Sector need to reevaluate risks regularly. These threats and hazards will likely increase as organisations within the Transport Sector become more technologically interconnected in their daily operations for convenience and efficiency purposes, establishing additional avenues for exploitation; for example, through cyber-connected smart meters and other automated technologies, and through interconnected supply chain providers. These dynamic considerations mean that stakeholders in the Transport Sector need to continuously reevaluate the risks from the cyber threat.






Understanding sector-specific risks

This table outlines a select example of identified threat and hazard vectors that impact Transport 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">ConfidentialityIntegrityAvailability	Countries seeking to disrupt Australia's critical infrastructure may use advanced persistent threats or other modus operandi to scope, exert influence or disable transport networks.
	Remote access to operational technology	<ul style="list-style-type: none">ConfidentialityIntegrityAvailability	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">IntegrityAvailability	If harnessed effectively, cyber attacks can be used to inform cyber sabotage attacks, to gain control of OT, indefinitely suspend or otherwise degrade capability.
	Financially-motivated cyber-crime	<ul style="list-style-type: none">ConfidentialityIntegrityAvailability	Ransomware deployed into the networks of energy 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">AvailabilityReliability	As experienced since 2020, pandemics such as COVID-19 have the potential to greatly alter the functioning of society, with developments such as higher demand for delivered goods placing the transport industry under snap operational change.
	Severe weather events	<ul style="list-style-type: none">AvailabilityIntegrityReliability	Energy infrastructure is likely to be impacted by more frequent extreme weather and natural disasters, causing physical damage to roads, ports and other transport infrastructure.

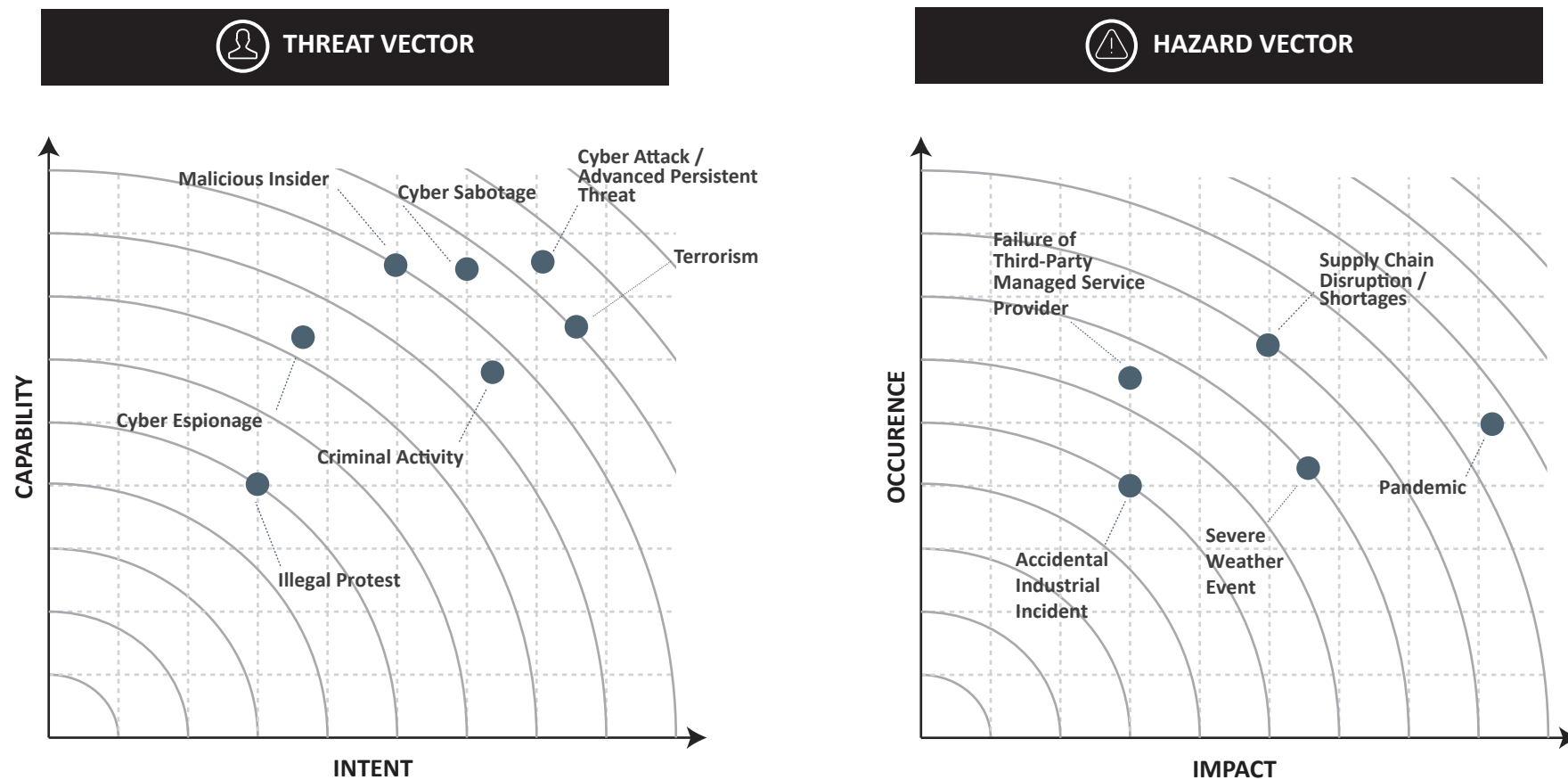


	Threat or Hazard Vector	Area of Potential Impact	Risk Scenario Considerations
 PHYSICAL	Terrorism	<ul style="list-style-type: none">ConfidentialityAvailabilityReliability	Groups that seek to make political statements through unlawful means may intentionally target infrastructure and assets critical to the Transport Sector to cause civil unrest or inflict casualties.
	Illegal Protest	<ul style="list-style-type: none">ConfidentialityAvailabilityReliability	Groups that seek to make political statements through unlawful means may intentionally damage or disrupt port, rail, road and other transport infrastructure.
 SUPPLY CHAIN	Extra-judicial actions by foreign powers	<ul style="list-style-type: none">IntegrityAvailabilityReliability	Foreign powers seeking to exert influence on the Australian economy may conduct sabotage or espionage or undertake direct extrajudicial actions to damage the Transport Sector
	Failure of third-party management	<ul style="list-style-type: none">AvailabilityReliability	Third parties relied upon to provide resources to the Transport Sector have the potential to fail, meaning that they cannot provide resources such as vehicle parts, fuel and fuel additives, disabling the transport asset downstream.
	Supply issues/ shortages	<ul style="list-style-type: none">IntegrityIntegrityReliability	Reliance on turbulent fuel market, the Transport Sector is vulnerable to outside forces. These forces may take the form of either market changes, or geopolitical manoeuvres, with Australia reliant on countries such as China for fuel additives.
 PERSONNEL	Malicious Insider	<ul style="list-style-type: none">ConfidentialityIntegrityAvailabilityReliability	A trusted insider has the ability to cause significant damage to critical infrastructure through deliberately disrupting critical components of a transport asset, physical damage intentionally, or disclosure of privileged information.
	Accidental industrial incident	<ul style="list-style-type: none">IntegrityAvailabilityReliability	Hazards, such as an accidental industrial incident can cause significant risk for a entity. An incident such as an improperly-controlled critical system could resulting in widespread transport network failures.

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 Transport 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:

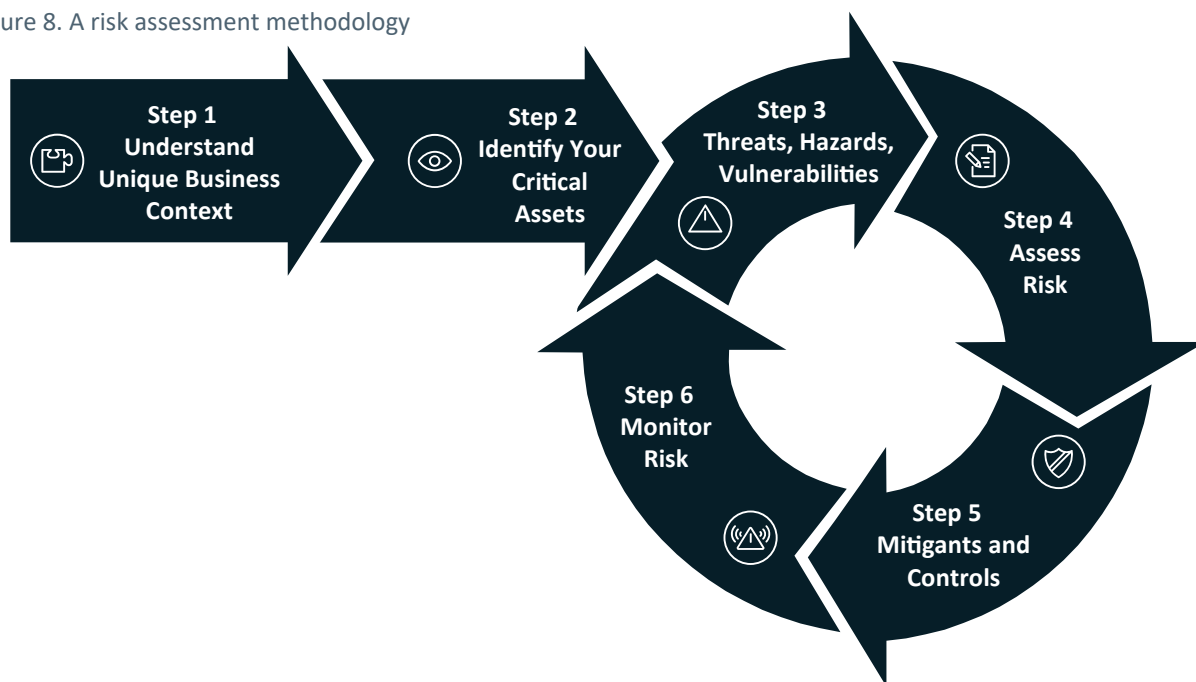
- Ease of implementation
- Cost-effectiveness
- Whether the action creates new risks and/or unintended consequences
- Environmental impacts (positive and negative)
- Multi-objective actions
- Long-term and short-term results
- Effectiveness
- Direct and indirect benefits
- Legal, regulatory, social and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



Appendix – A risk assessment methodology

Transport 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 Transport 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.