



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

Essential for a functioning society – via the outputs used to maintain quality life for citizens, or to the Energy Sector's contribution to the economy.

Reliant on industrial control systems and operational technology – with an increasing push towards remote management.

Critical to national security – as a supporting sector for every other sector within Australia.

Susceptible to cyber attack – dated infrastructure is susceptible to damage that may take entire grids and systems offline, disabling other sectors.

Subject to regular changes in regulation – which often impact operational processes and infrastructure management.

Significant use of third- and fourth-party relationships – integrated in multiple business processes, which creates exposure to external threats through these relationships.

Increasing use of innovative Internet of Things (IoT) technologies – such as smart meters, and drones.

Susceptible to investment changes – where investment can be influenced by multiple external forces, including the politics of the day.

Susceptible to reliability impacts – where unreliable assets can drastically reduce operating efficiency.

High availability requirements – often focused within a number of pinch-points or single points of failure.



Risk in the critical infrastructure context

Identifying risk for critical infrastructure

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

An example of how to identify this risk for the Energy Sector is framing a possible risk from the loss of control of operational technology (such as a programmable logic controller that operates a valve of a gas facility), as to how it may disrupt the availability of domestic gas supply, as well as the impact on the grid's critical downstream customers who have a dependence on the site's contribution of domestic gas.

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

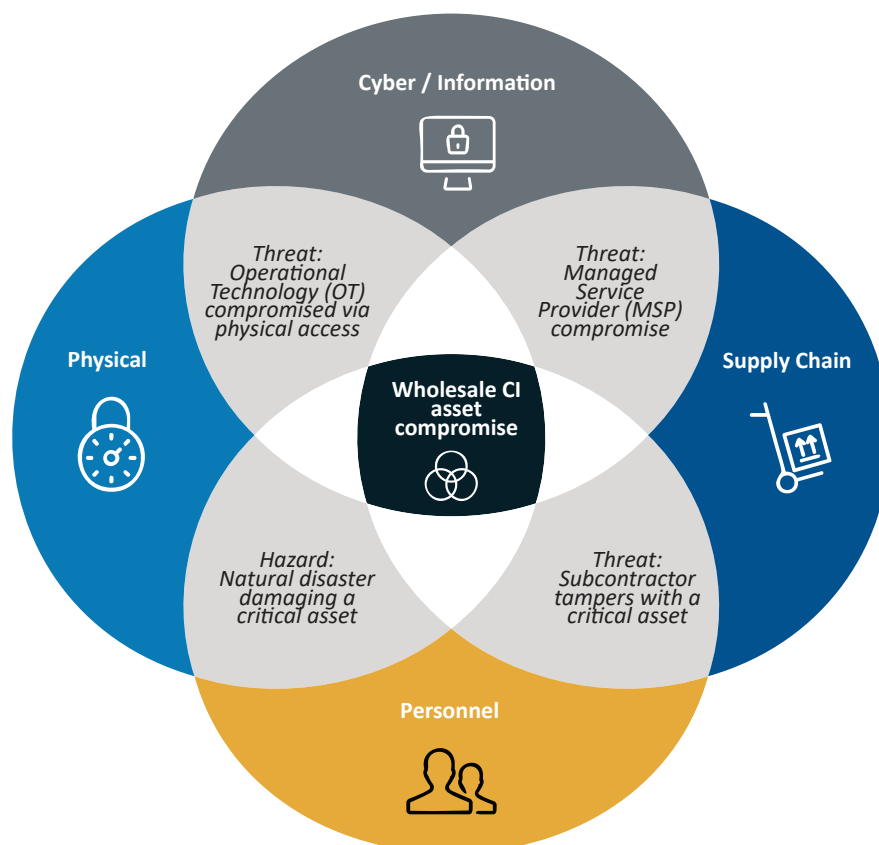
Some entities in the Energy Sector have security-related regulations already in place. Entities in the sector may need to consider guidance such as the Australian Energy Sector Cyber Security Framework (AESCSF) or the Australian Domestic Gas Security Mechanism (ADGSM), or look to their state or territory 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:

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

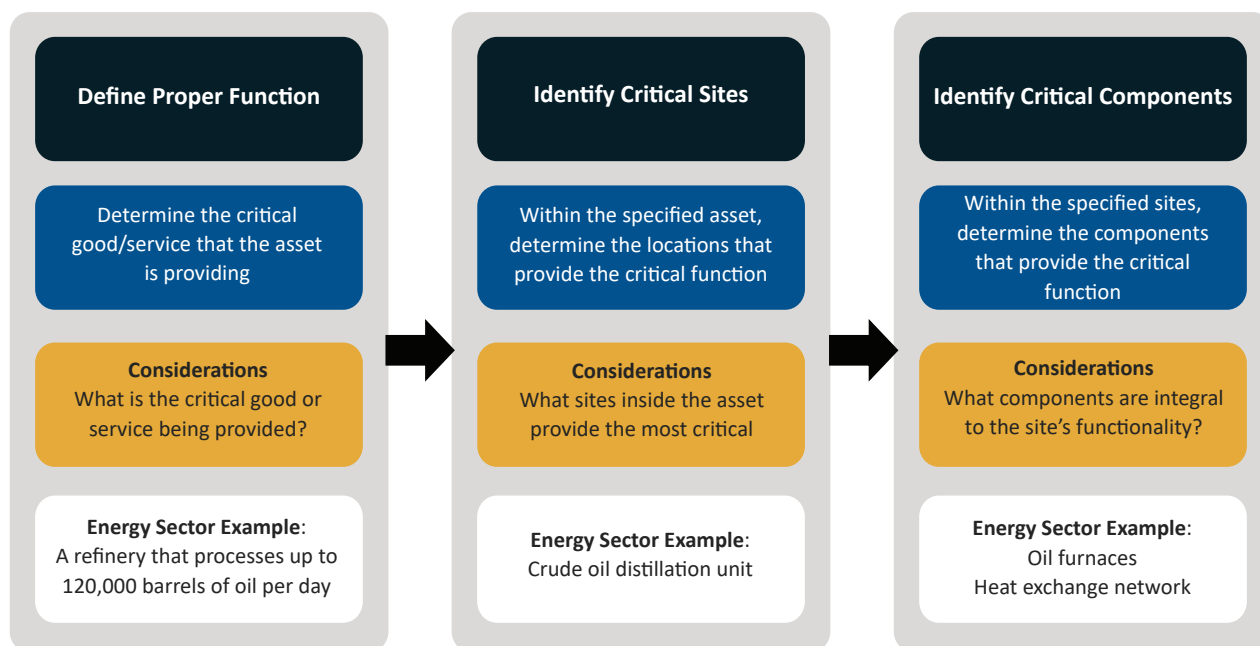
- (a) the production, transmission, distribution or supply of electricity; or
- (b) the production, processing, transmission, distribution or supply of gas; or
- (c) the production, processing, transmission, distribution or supply of liquid fuel.

Identifying and assessing criticality

For Energy 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, according to the SOCI Act an interconnector is critical if it provides energy to 100,000 customers. The proper function of this asset may be compromised if it is unable to deliver energy to customers.

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

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

Critical components are those required to maintain the function of the asset, or whose absence, compromise or damage could cause significant harm to the asset. For an energy organisation, a critical component may include transmission wires that allow energy to be distributed to customers, or a component such as a valve or programmable logic controller that allows gas to be distributed from one storage vessel to another.



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 Energy Sector:

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

Emerging Trends

- **Exploring distributed energy resources:** Battery storage, advanced inverters and solar photovoltaics both behind and in front of the meter.
- **Improving asset management:** Field service mobility, works management and remote inspection technologies, such as drones.
- **Exploring mini-grids and micro-grids:** Integrating distributed energy resources with advanced monitoring, communications and control systems.
- **Developing advanced analytical tools:** Enabling forecasting and supporting real-time decision making.
- **Deprecation of fossil fuel use:** replacement of traditional energy sources with renewable and/or alternative energy sources.
- **Significant physical transformation:** Transition of infrastructure to support the operation of renewable forms of electricity, the storage of electricity through advances in battery storage, and the transmission of energy outputs of renewable energy generation.
- **Desire to increase liquid fuel stockpiling:** To reduce short-term dependence on liquid fuel supply.
- **Disruption to liquid fuel supply and demand:** From a demand perspective this is changing because of lockdowns and remote work in response to the COVID-19 pandemic and, from a supply perspective, is susceptible to geopolitical changes and depletion of natural resources.

Emerging Technology

- **Storage:** Declining lithium battery prices in recent years has increased the rollout speed of green solutions. Lithium battery technology has allowed for more efficient energy storage and versatile use of battery technology.
- **Sector integration:** Improved deployment of green technology with large-scale battery storage facilities has facilitated effective use of renewable energy sources.
- **Artificial intelligence:** Deployed to implement predictive maintenance of wind and solar arrays.
- **Hydrogen:** Investment in hydrogen has meant that industry research and growth is increasing.
- **Carbon capture technology:** Gaining traction as a method to offset industry carbon footprints.
- **Waste-to-energy technology:** Research and emerging infrastructure to make use of landfill to produce energy.
- **Low emissions heat systems:** Methods of producing heat with low emissions such as solar thermal, heat pumps and hybrid systems, in mining and manufacturing.



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/>



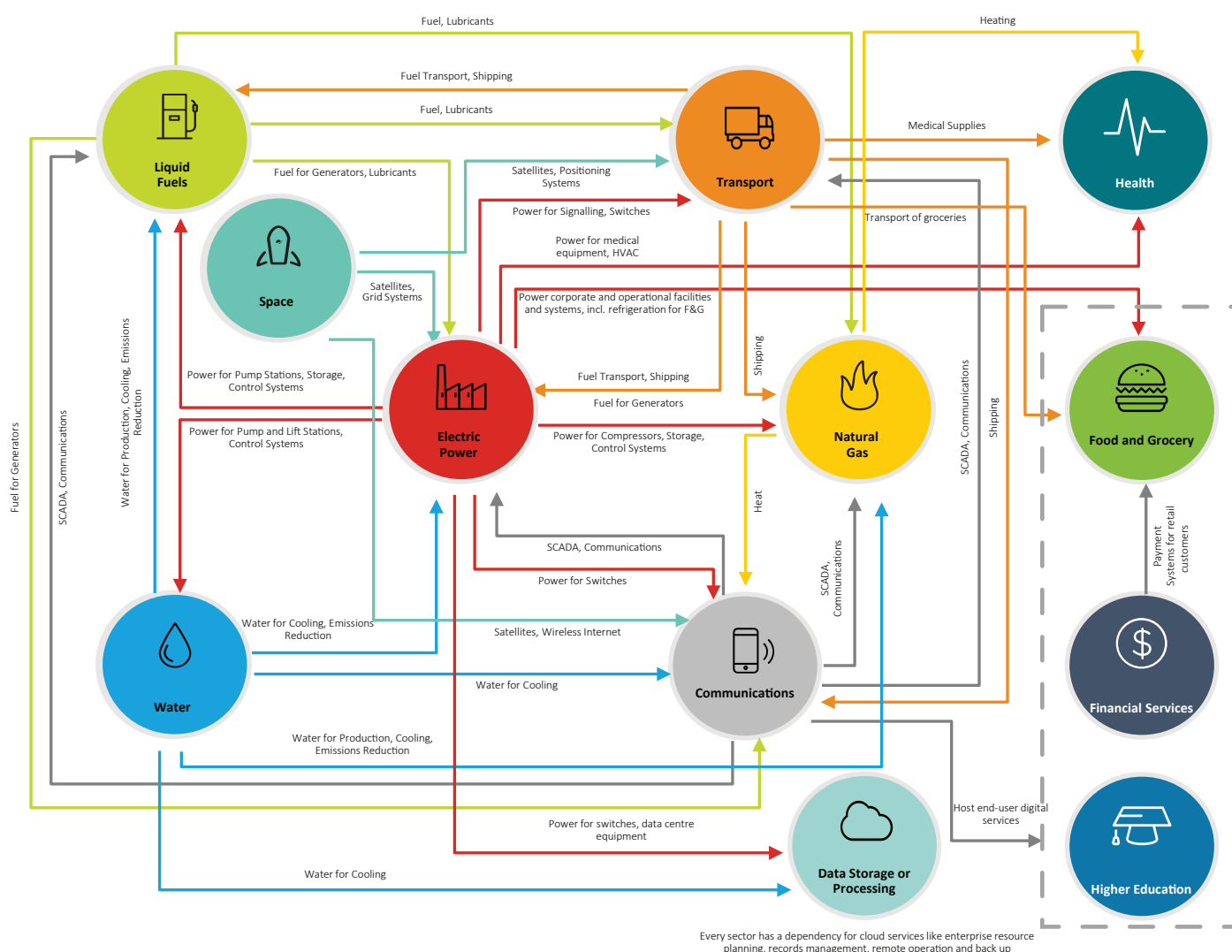
Interdependencies (upstream and downstream)

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 Energy 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.

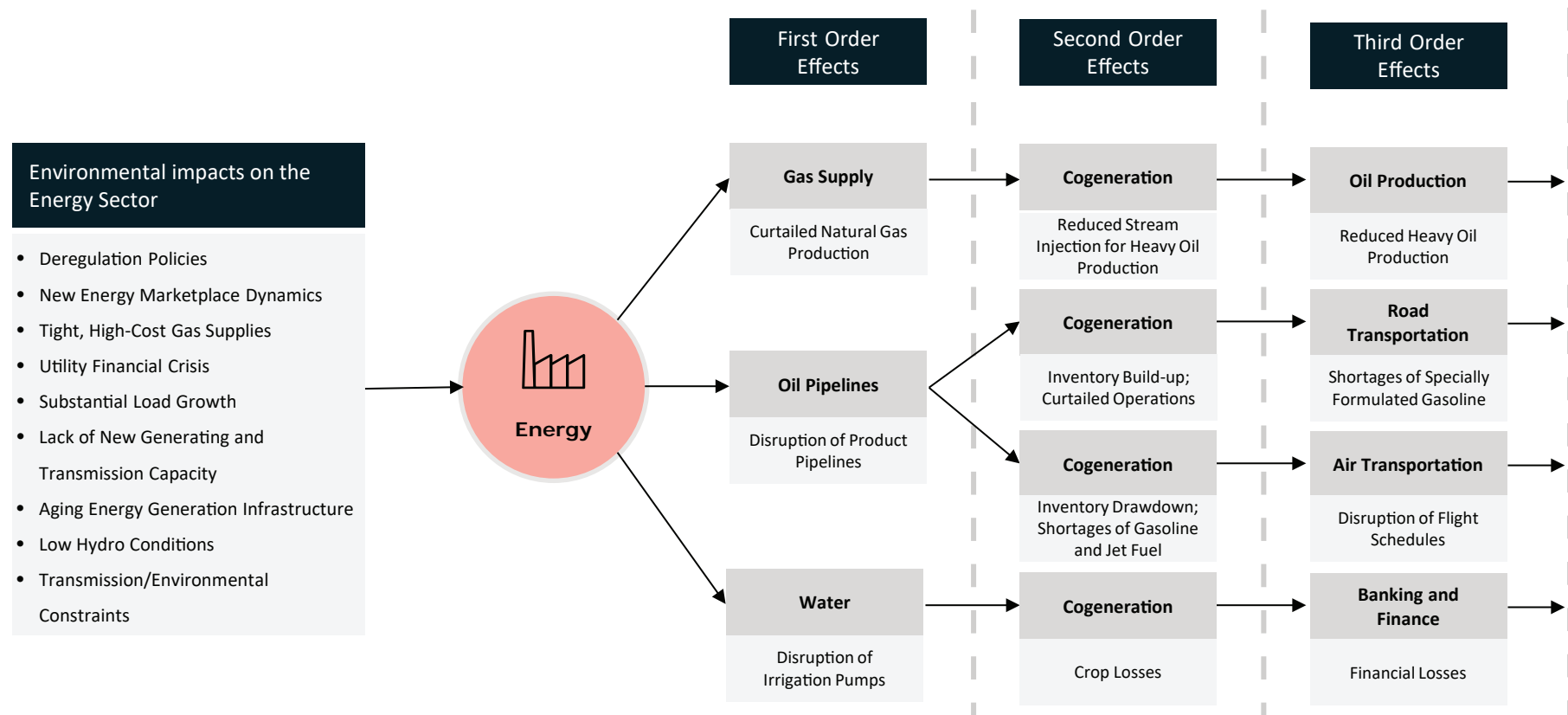
Figure 4. An example of sector interdependencies and relationships



Flow-on effects for relevant impacts against Energy 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 Energy Sector.

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





An outage affecting a critical asset in the Energy Sector could result in significant economic or societal implications. Impacts could be significant in severity, depending on the geographic breadth of the outage and the effect on the broader supply of energy. For example:

- While hospitals typically have backup generators and battery backups, customers in residential areas may not have redundant infrastructure, and a loss of power to life-support devices may result in loss of life. In 2016, three energy suppliers were fined a total of AUD120,000 for allegedly cutting power in planned outages without appropriately warning customers who require life support.
- In 2016, a business survey held the cost to the South Australian economy following the widespread power outage to be in the order of AUD367 million, or close to AUD120,000 per minute for business in the state.
- Unauthorised changes to infrastructure may have the potential to result in overload, surges or electricity arcing, having the potential to damage infrastructure and to create safety hazards.
- Financial impacts may include litigation and infringement costs as a result of service impacts to clients and increased market costs for energy, especially if cheaper energy sources are compromised and more expensive sources are required to sustain the same level of market generation contribution.
- Impacts to liquid fuel and gas assets, systems, and/or elements could cause additional service outages, such as fuel shortages impacting motor vehicles, aircraft, and fuel-dependant systems (i.e. generators). These shortages may cause cascading outages in the transport sector, which has a heavy reliance on gas and liquid fuel; this, in turn, could cause wide-ranging cascading failures in other industries that rely on the transport sector, such as tourism, supply and logistics, immigration, and public transport and consumer vehicles.

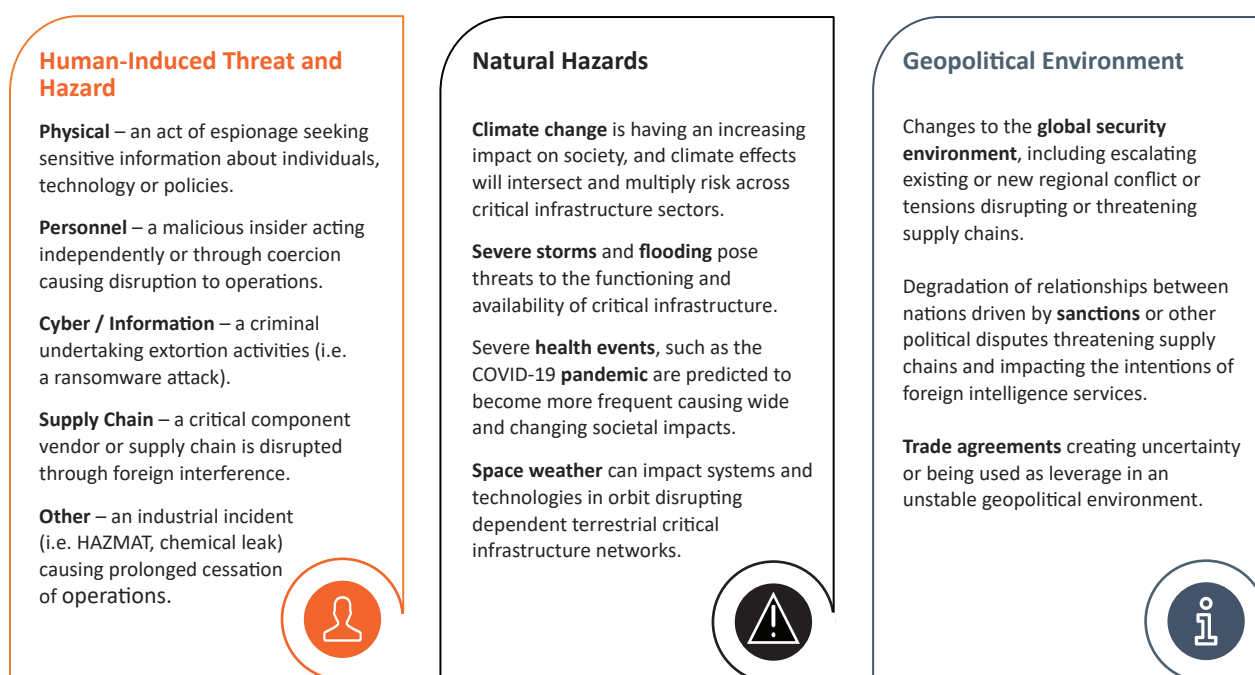


Understanding threats and hazards for risk

Identifying a threat and hazard landscape of the Energy Sector

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

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



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

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



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

Natural hazards are becoming more frequent and intense, and their impacts enduring and complex. The Energy Sector is especially susceptible to these risks due to its use of dangerous materials and sensitive technology.






Understanding sector-specific risks

This table outlines a select example of identified threat and hazard vectors that impact Energy 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 and disable energy generation and/or transmission to create disruption or cessation of energy delivery to the grid.
	Cyber-espionage	<ul style="list-style-type: none">ConfidentialityIntegrityAvailability	Cyber espionage could be used to exfiltrate, monitor, intercept and manipulate data pertaining to energy control systems and, current and future capabilities.
	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 energy in residential areas.
	Space weather event	<ul style="list-style-type: none">ConfidentialityAvailabilityReliability	Geomagnetic storms from space weather events could impact power supply directly via transformer and other infrastructure damage, and indirectly by impacting the availability of communications equipment.
	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 damage or delay to the output from the sector.

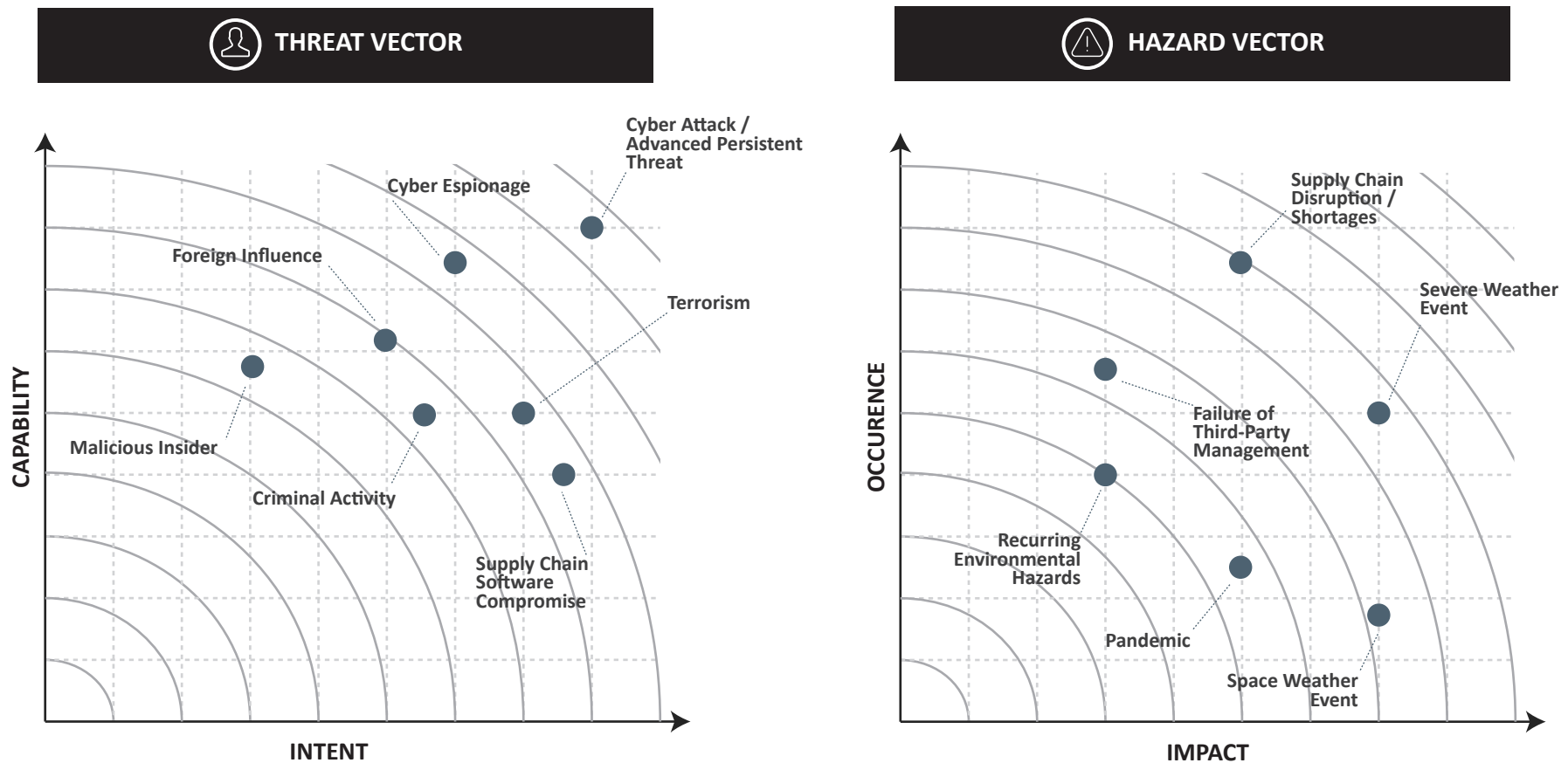


	Threat or Hazard Vector	Area of Potential Impact	Risk Scenario Considerations
 PHYSICAL	Foreign Interference	<ul style="list-style-type: none">ConfidentialityAvailabilityReliability	Foreign ownership in Australia's energy generation and transmission may be subject to interference from foreign adversaries, using access or coercion to cause disruptions.
	Terrorism	<ul style="list-style-type: none">ConfidentialityAvailabilityReliability	Groups that seek to make political statements through unlawful means may intentionally damage power plants, grids and wider networks to cause civil unrest.
 SUPPLY CHAIN	Supply issues/shortages	<ul style="list-style-type: none">ConfidentialityAvailabilityReliability	The compromising of a coal supplier's network may infect an energy provider, causing downstream damages and flow-on effects.
	Failure of third-party management	<ul style="list-style-type: none">AvailabilityReliability	Failure by third parties to deliver resources relied on by Energy Sector assets could affect other critical infrastructure assets downstream, who rely on the energy providers.
	Foreign Interference in supply chain by extra-judicial actions	<ul style="list-style-type: none">ConfidentialityIntegrityReliability	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">ConfidentialityIntegrityAvailabilityReliability	A trusted insider has the ability to cause significant damage to critical infrastructure such as deliberately disclosing privileged information or manipulating technology used by assets with the intent to cause harm.
	Accidental industrial incident	<ul style="list-style-type: none">IntegrityAvailabilityReliability	Hazards, such as an accidental industrial incident can cause significant risk for a entity. For the Energy Sector, an incident such as an improperly-controlled critical system could resulting in operational failure.

Prioritisation of sector threats and hazards

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

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



Source: Deloitte Risk Advisory and Cyber and Infrastructure Security Centre



Risk controls and mitigations

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

For a given Energy 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 energy 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:

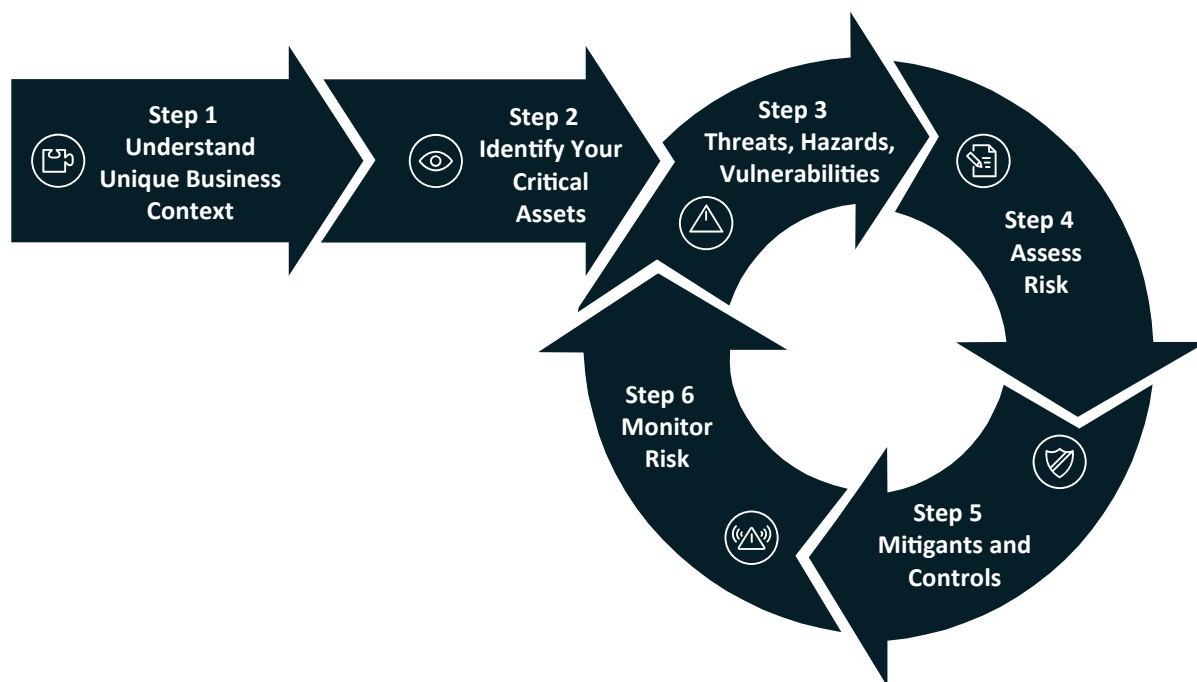
- Ease of implementation
- Cost-effectiveness
- Whether the action creates new risks and/or unintended consequences
- Environmental impacts (positive and negative)
- Multi-objective actions
- Long-term and short-term results
- Effectiveness
- Direct and indirect benefits
- Legal, regulatory, social and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



Appendix – A risk assessment methodology

Energy 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 Energy 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.