



Risk Assessment Advisory for Critical Infrastructure

Food and Grocery 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 Food and Grocery 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 **Food and Grocery Sector** are outlined below:

Critical to Australian prosperity – in keeping Australians fed, and as a contributor to the economy through imports and exports.

Susceptible to environmental forces – which can result in destruction of crops before harvesting, in storage or in transport.

Some aspects are highly regulated – strict safety standards to protect food from contamination and to maintain its quality in transit/storage.

Dependence on large labour resources – both grocers and farmers are employers of primarily young, high-turnover, seasonal workforces.

Source of origin and ethical traceability are a key focus – for consumers who are mindful of where their goods come from and how they move through the supply chain, particularly where international producers or processors are concerned.

Increasing use of new technology – for providing transparency in the supply chain, and artificial intelligence for growing, harvesting, processing, and distribution of food; as well as in the supply chain from harvesting to shelves.

Food security an ongoing concern – as Australia's population grows and is subject to geopolitical headwinds impacting supply chains.

Time-sensitive – many types of foodstuffs are perishable in nature.

Specialist transport needs – including refrigeration of goods, particularly in the dairy and meat segments.

Collaboration with foreign entities – is required to maintain international supply chains for both imports and exports

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 the Food and Grocery Sector is framing a possible risk from a prolonged power outage in a major food storage warehouse caused by a natural disaster (i.e. severe weather or earthquake) affecting the distribution of a limited available, critical food or grocery item to national markets.

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

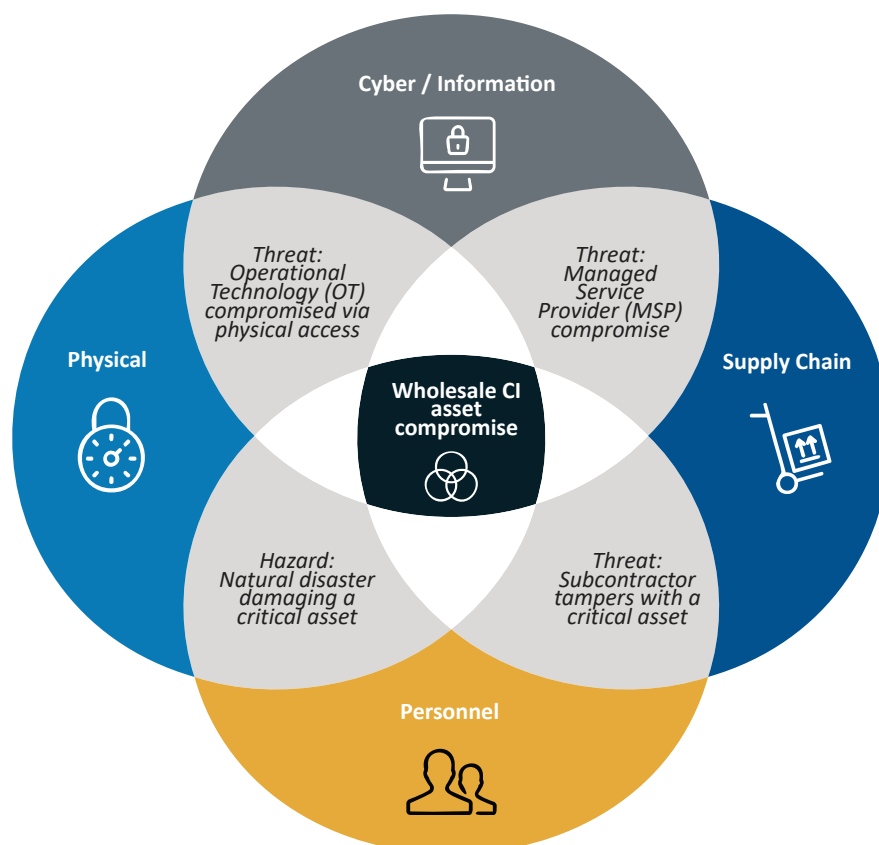
Some entities in the Food and Grocery Sector have security-related regulations already in place. Entities in the sector may need to consider guidance such as the Australia New Zealand Food Standards Code, the Food Safety Act 1991, or look to their state or territory governments for regulatory frameworks 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:

food and grocery sector means the sector of the Australian economy that involves:

- (a) manufacturing; or
- (b) processing; or
- (c) packaging; or
- (d) distributing; or
- (e) supplying.

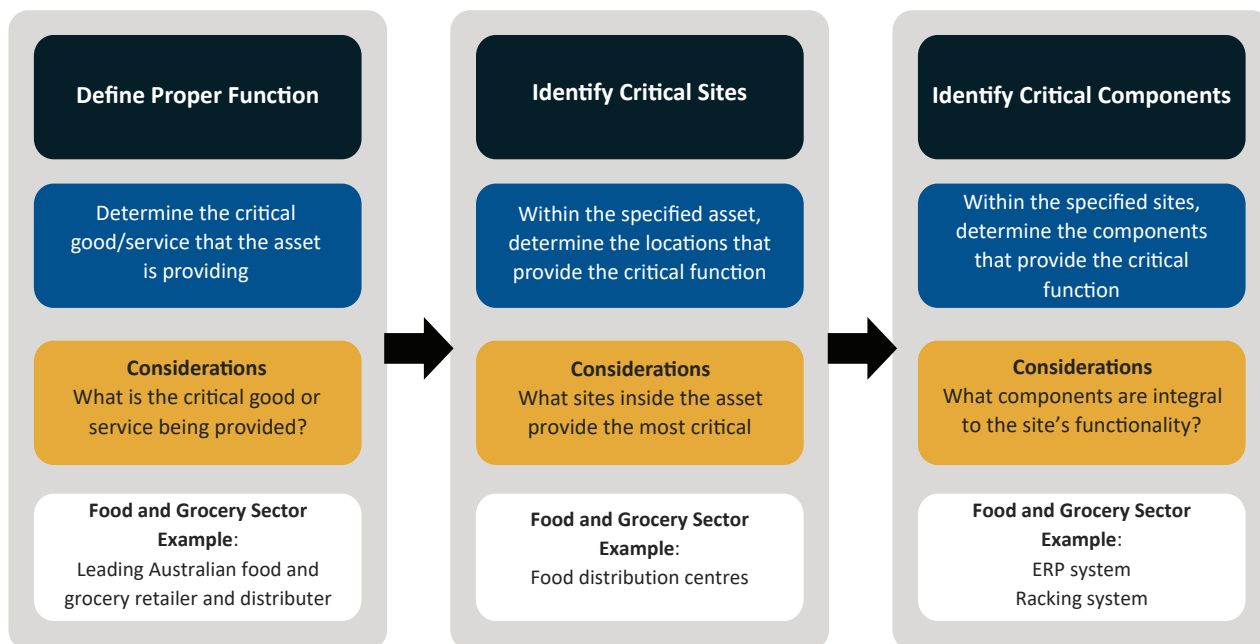
food and groceries on a commercial basis.

Identifying and assessing criticality

For Food and Grocery Sector critical infrastructure providers, determining which sites and components of an asset should be considered critical involves identification and analysis of how an asset and its operations may be exposed to, or harmed by, threats and/or hazards. This process is vital for all hazards risk management, providing input into the identification of plausible risk scenarios that may impact operations. The critical sites and components of an asset are ultimately those most vital to its effective functioning and therefore integral to Australia's national security interests. Establishing criticality is designed to provide guidance on the allocation of resources to best protect the operational capability of the asset.

The 'responsible entity' for an asset is able to determine the extent of this activity; however, a suggested process using a select example is outlined below.

Figure 2. Example of determining criticality of an asset



A function of a critical infrastructure asset may be the provision of a critical good or service that is a contributor to the economic or social wellbeing, defence, or security of the nation.

For example, a large supermarket chain has been identified as critical due to its integral role within Australian food distribution. The proper function of this asset is defined as being able to distribute food and groceries to customers.

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 appreciate the level of criticality.

Critical sites are those in which assets assigned proper functions are located. This could include corporate head offices, warehouses, or other areas based on the context of the specific asset.

The responsible entity of a critical infrastructure entity 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 anything that is required to maintain the function of the asset, or whose absence, compromise or damage could cause significant harm to the asset. For a food and grocery organisation, critical components may include an enterprise resource planning system that manages day-to-day business activities, such as supply chain operations, or refrigeration systems that maintain perishable goods.



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 Food and Grocery Sector:

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

Emerging Trends

- **Changes in local and international demand:** Constantly shifting needs of the supply chain, increasing or decreasing demand on areas like packaging, manufacturing and, transport and logistics.
- **Traceability and ethical sourcing:** Increasingly a concern for consumers, requiring more transparency from the Food and Grocery Sector as to where commodities are sourced from and how they move through the supply chain.
- **Increasing demand for online shopping:** Changing the ways in which consumers shop and how food and groceries reach consumers. While this can reduce demand for bricks-and-mortar supermarkets, it can increase demands on other parts of the supply chain, such as wholesalers and distributors. This also increases demand for the manufacture and supply of packaging, particularly where goods are perishable, individualised or fragile.
- **Short-term demand for 'Dark Stores' overtaken by larger players:** Bricks-and-mortar stores, originally functioning as supermarkets or grocers, were converted into e-commerce packing, warehousing and distribution centres to maintain supply during COVID-19 pandemic. Post-pandemic demand for online shopping is expected to remain high, inviting larger players to consider transforming parts of their operations to a 'Dark Store' model.

Emerging Technology

- **Innovation driving large-scale change:** In an industry that has historically relied more on labour force than technology, many organisations are innovating or embedding new processes to reduce workforce overhead, increase automation of tasks like packaging and distribution, and to reduce time to market.
- **Transition to cloud services:** This is happening throughout the supply chain for a range of data processing activities. Vast quantities of information about how consumers shop, including shopping preferences, statistics and the use of loyalty programs, are being captured, stored and analysed to provide supply and demand, and marketing insights; much of this is processed in the cloud.
- **Robotics in AI in picking and packing:** Increasing in use, with automation in farming, irrigation, harvesting, quality inspection, packaging and distribution becoming increasingly common. This can create efficiencies in the supply chain, but also has the potential to disrupt the market and workforce. This is also a potential disrupter from international producers who integrating automation faster than local producers.



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/>



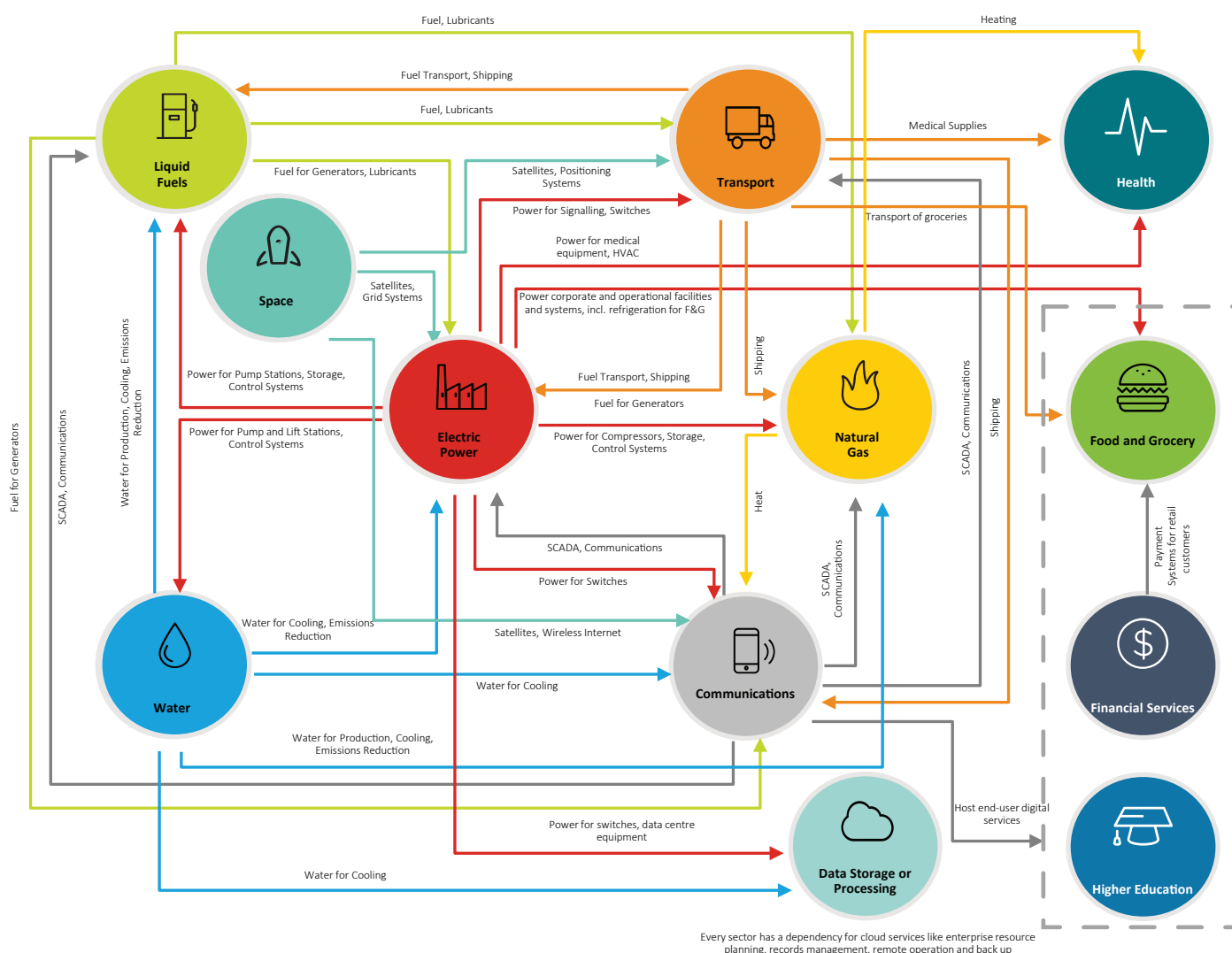
Interdependencies (upstream and downstream)

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 Food and Grocery 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

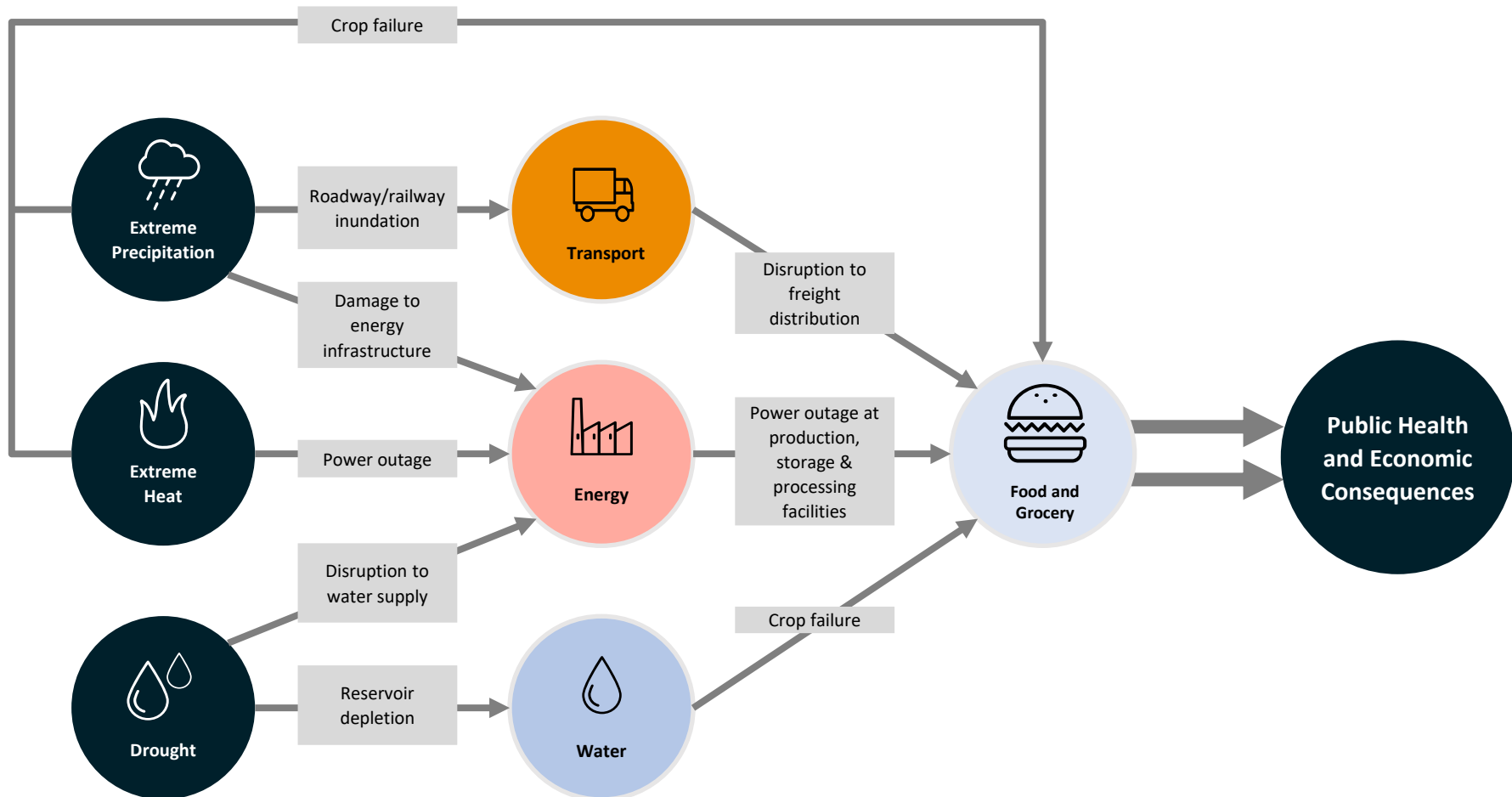




Flow-on effects for relevant impacts against Food and Grocery Sector assets

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 Food and Grocery Sector.

Figure 5. Example of flow-on effects from an impact against the Food and Grocery Sector





Dependent on the asset, system, and/or network could have significant economic and/or societal implications, depending on the asset, system or network affected. Impacts could be significant in their severity, depending on the geographic breadth of the outage, and the detriment of the impact to the broader water network. For example:

- In September 2018, news reports confirmed that strawberries provided by a range of brands grown in Queensland and Western Australia had been contaminated by a malicious actor inserting needles into them. This resulted in at least one case of a consumer being hospitalised for emergency care, and caused mass recalls of strawberries across Australia, doing major damage to consumer confidence in the supply chain. While contamination in the supply chain may be limited to only one or two brands, it has a profound effect on consumer confidence.
- With the supply chain reliant on its collective moving parts working in a smooth and timely fashion, the sector is vulnerable to disruption from industrial action. There have been multiple incidents where industrial action has resulted in shortages or spoilage of perishable goods, particularly in logistics and distribution elements of the supply chain.
- Long years of drought have resulted in multiple instances of large-scale livestock death from dehydration, demonstrating the sector's reliance on water storage and distribution, as well as the supply of grain and livestock feed. These livestock deaths have results in fines in the tens of thousands of dollars, notwithstanding the associated financial losses and reputational damage.
- Food and grocery contamination is monitored by Australian Government organisations, which set high standards for the sector; even the potential for contamination through microbial contamination (salmonella, listeria), physical contamination (plastics, glass), or animal contamination (hairs, faeces) can trigger a localised or nation-wide product recall. This can result in disruptions to the supply chain through investigation and review, as well as financial loss from unsold goods.
- Outages of point-of-sale systems, which can occur for a variety of reasons including loss of communications or errors in operating software, can effectively shut down the operations of an entire store chain, resulting in loss of revenue and reputational damage.

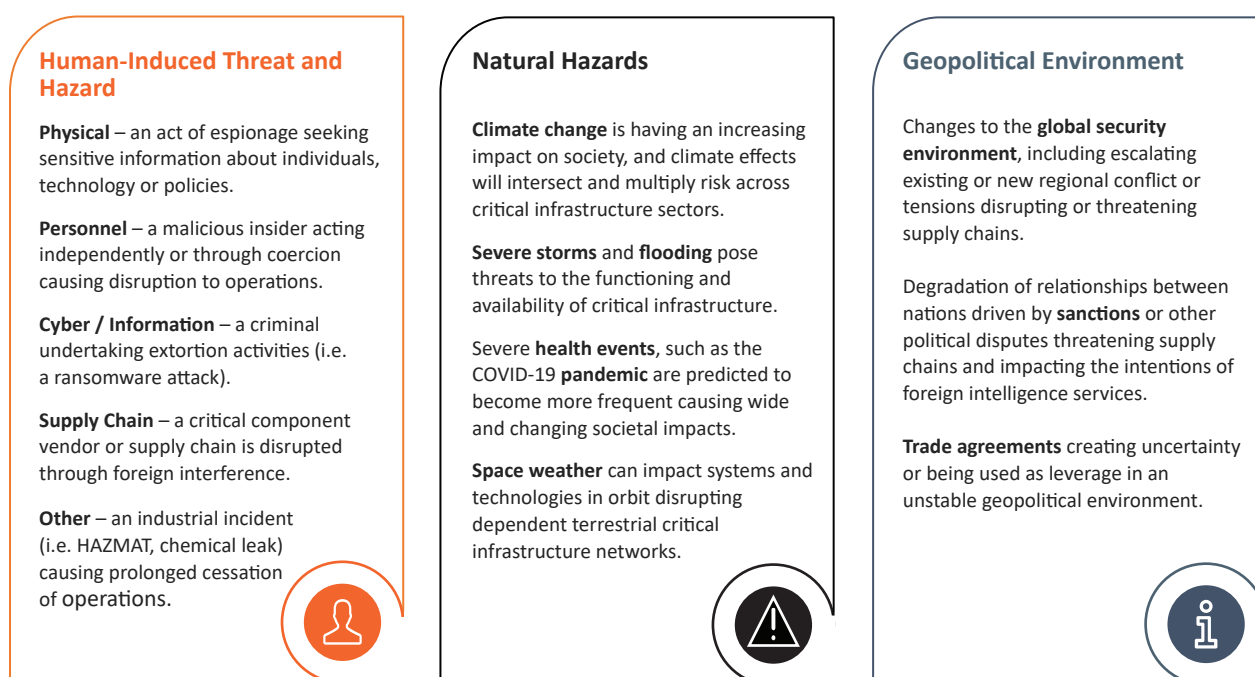


Understanding threats and hazards for risk

Identifying a threat and hazard landscape of the Food and Grocery Sector

All-hazards risk assessment considers both human-induced and natural threats and hazards. Given its role in critical infrastructure, the Food and Grocery Sector is an attractive target for threat actors seeking societal disruption; and natural hazards can severely damage the infrastructure and the food itself. 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 Food and Grocery Sector, driven by improvements in technology and the need to meet commercial outcomes, will become more interconnected. This means that stakeholders in the Food and Grocery Sector need to reevaluate risks regularly.

Natural hazards are becoming more frequent and intense, their impacts enduring and complex. The Food and Grocery Sector is susceptible to these kinds of hazards through damage to facilities, componentry, and impacts to food quality.






Understanding sector-specific risks

This table outlines a select example of identified threat and hazard vectors that impact Food and Grocery 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	Risk Scenario Considerations
 CYBER / INFORMATION	Foreign interference	<ul style="list-style-type: none"> Confidentiality Integrity Availability <p>Countries seeking to disrupt Australia's critical infrastructure may use advanced persistent threats or other modus operandi to scope, exert influence or attempt to disrupt critical food supply chains.</p>
	Cyber-espionage	<ul style="list-style-type: none"> Confidentiality Integrity Availability <p>Cyber espionage could be used to exfiltrate, monitor, intercept and manipulate data pertaining to food distribution networks and, current and future capabilities.</p>
	Financially-motivated cyber-crime	<ul style="list-style-type: none"> Confidentiality Integrity Availability <p>Ransomware deployed into the networks of food and grocery providers has the potential to halt the functioning of an asset for extended periods with the intent to extract financial benefits.</p>
	Access vectors into networks	<ul style="list-style-type: none"> Confidentiality Integrity Availability <p>Due to the interconnected nature of food and grocery assets, remote technology is often used to access and manage them (inventories, organise other logistics); this can be exploited by malicious actors to gain quick and easy access to critical systems.</p>
 NATURAL	Pandemic	<ul style="list-style-type: none"> Confidentiality Availability Reliability <p>Pandemics such as COVID-19 have the potential to greatly alter the functioning of society, with developments such as higher demand for specific items (such as toilet paper) creating major supply disruption.</p>
	Severe weather event	<ul style="list-style-type: none"> Availability Reliability <p>With increasing extreme weather events, people in affected areas may experience difficulties in accessing cash and other payment systems, which could be compounded if weather impacts impede access to affected areas.</p>

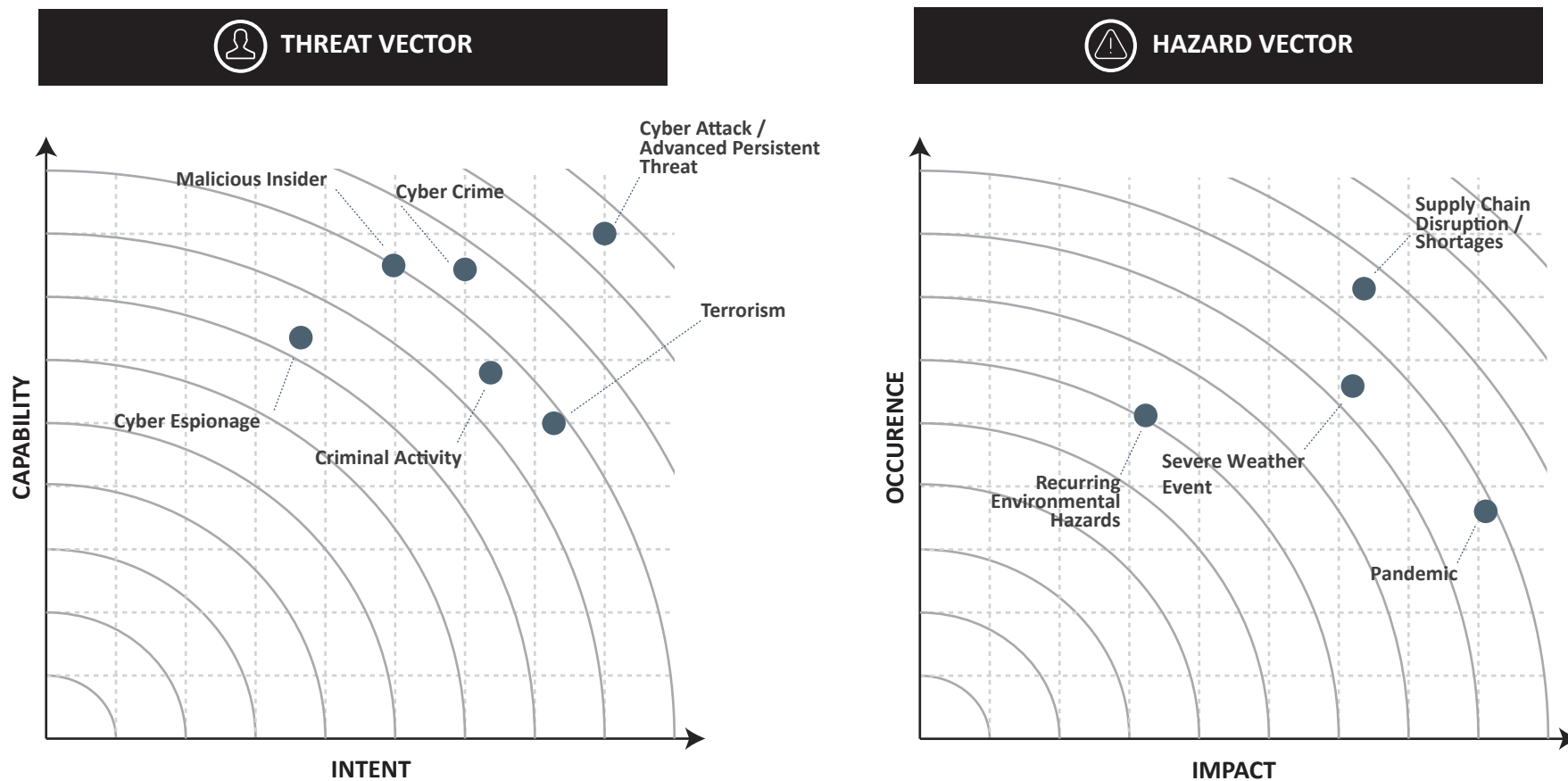


	Threat or Hazard Vector	Area of Potential Impact	Risk Scenario Considerations
 PHYSICAL	Criminal activity	<ul style="list-style-type: none">• Integrity• Availability• Reliability	Criminal activity can cause damage through fraud, theft or coercion. These criminal activities can have broader consequences such as reputational damage and loss of income.
	Terrorism	<ul style="list-style-type: none">• Confidentiality• Availability• Reliability	Groups that seek to make political statements through unlawful means may intentionally damage food distribution or contaminate products.
 SUPPLY CHAIN	Supply issues/shortages	<ul style="list-style-type: none">• Confidentiality• Availability• Reliability	The reliance of the sector upon third parties for supply and services means indirectly these entities can have a significant affect the functioning of food supply and distribution.
	Failure of third-party management	<ul style="list-style-type: none">• Availability• Integrity• Reliability	Supplies provided by foreign may be affected by international sanctions, and even if components are available Australian communication entities may not be able to purchase needed components.
	Foreign Interference in supply chain by extra-judicial actions	<ul style="list-style-type: none">• Confidentiality• Integrity• Reliability	Supplies 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.
	Foreign ownership of domestic primary producers	<ul style="list-style-type: none">• Availability• Integrity• Reliability	Potential risk of disruption to the availability and reliability of food and grocery assets if there are unhelpful directions from foreign government interests
 PERSONNEL	Malicious Insider	<ul style="list-style-type: none">• Confidentiality• Integrity• Availability• Reliability	A trusted insider has the ability to cause significant damage to critical infrastructure such as deliberately disclosing privileged information or manipulating system used by assets with the intent to cause harm. For the Food and Grocery Sector, malicious insiders may seek monetary gain by intentionally contaminate a food stuff or grocery items.

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 Food and Grocery 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:

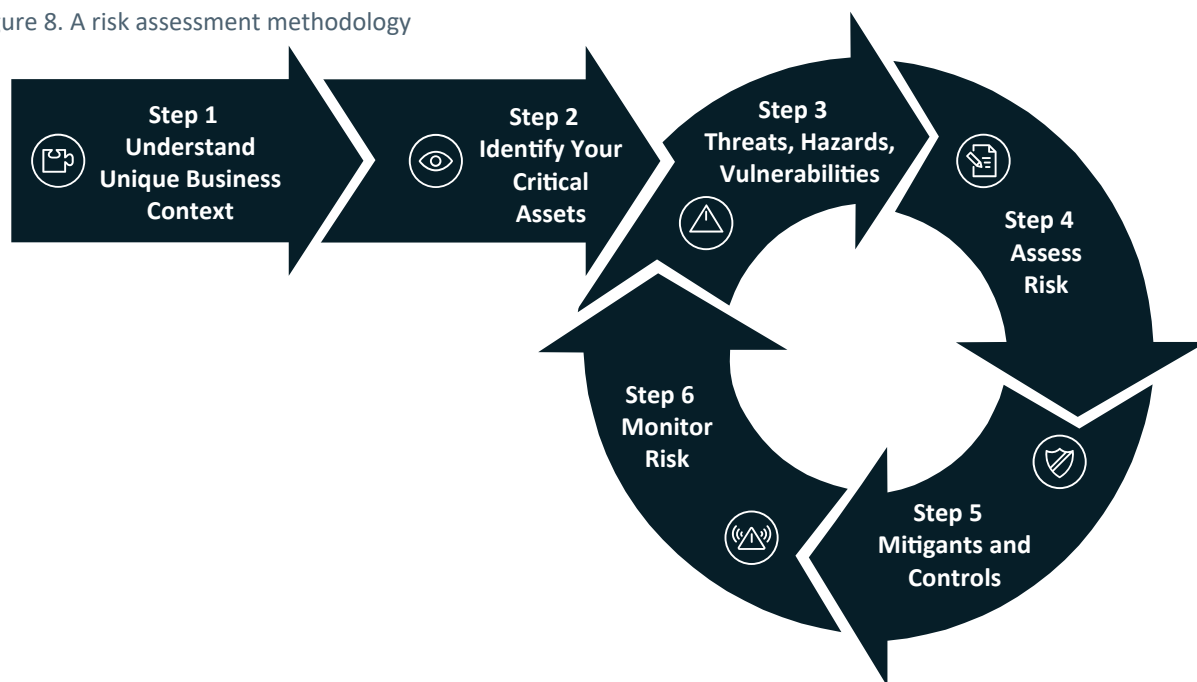
- Ease of implementation
- Cost-effectiveness
- Whether the action creates new risks and/or unintended consequences
- Environmental impacts (positive and negative)
- Multi-objective actions
- Long-term and short-term results
- Effectiveness
- Direct and indirect benefits
- Legal, regulatory, social and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



Appendix – A risk assessment methodology

Food and Grocery 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 Food and Grocery 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.