



## Risk Assessment Advisory for Critical Infrastructure Water and Sewerage 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 Water and Sewerage 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 **Water and Sewerage Sector** are outlined below:

**Wide use of Internet of Things (IoT) and SCADA systems** – to monitor and control water treatment, quality and distribution.

**Produce intellectual property** – through investment and innovation in water delivery and treatment.

**Long-life infrastructure** – some of which may not be network-capable.

**Targeted by multiple cyber attack actors** – particularly those motivated to cause disruption.

**Uses and produces toxic substances and hazardous materials** – in the treatment of effluent, and as a by-product of treatment. Environmentally conscious on concerns of water contamination or sewerage release.

**Highly regulated** – to maintain water quality for health, safety, and affordability of clean drinking water.

**Susceptible to physical attacks** – both through physical damage and networked physical infrastructure.

**Uses and produces toxic substances and hazardous materials** – in the treatment of effluent, and as a by-product of treatment.

**Susceptible to attacks launched through third parties** – including supply chain providers and contractors.

**Uses and produces toxic substances and hazardous materials** – in the treatment of effluent, and as a by-product of treatment.



## 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 Water and Sewerage Sector is framing a possible risk from a disruption to the supply of critical water-treatment chemicals, which in turn affects the reliability of water-treatment facilities and the availability of essential potable water to other highly-dependent critical infrastructure assets, such as those in the Healthcare and Medical Sector (i.e. hospitals).

### 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 their operations. Australia's critical infrastructure risk environment continues to evolve and an all-hazards approach is best placed to consider the potential convergence of the wide-ranging threats and natural hazards that could result in competing and cascading effects on national resilience.

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

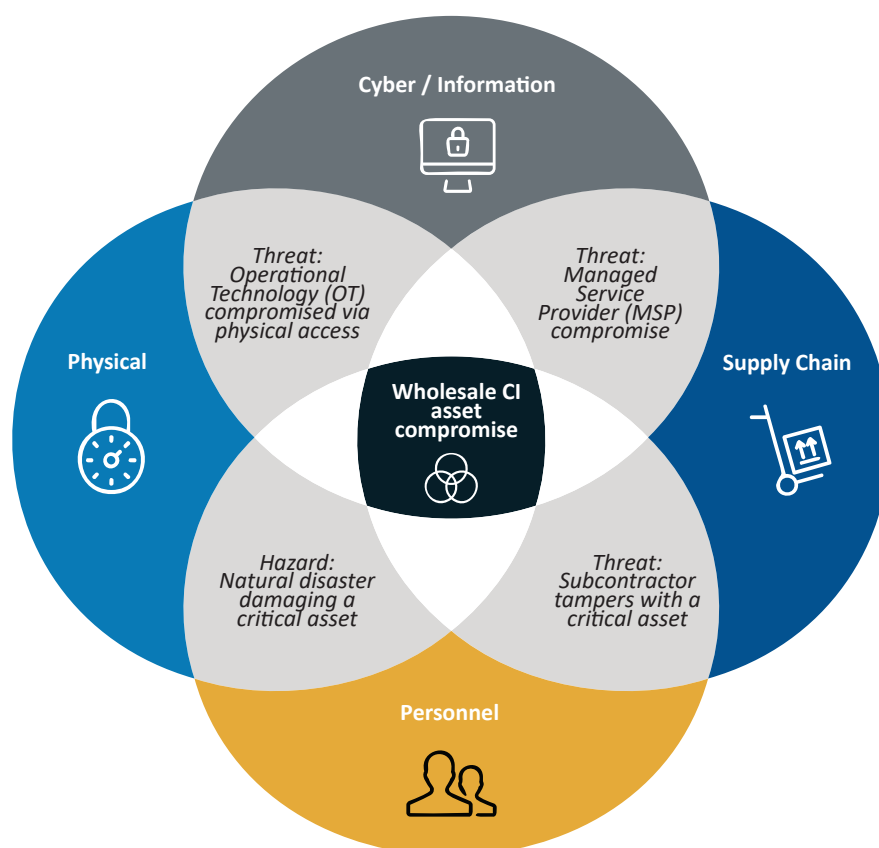
Some entities in the Water and Sewerage Sector have security-related regulations already in place. Entities in the Sector may need to consider guidance such as the Water Act 2007, or look to their state or territory government for regulatory frameworks and consider how they can incorporate national security-related 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:*

Water and sewerage sector means the sector of the Australian economy that involves:

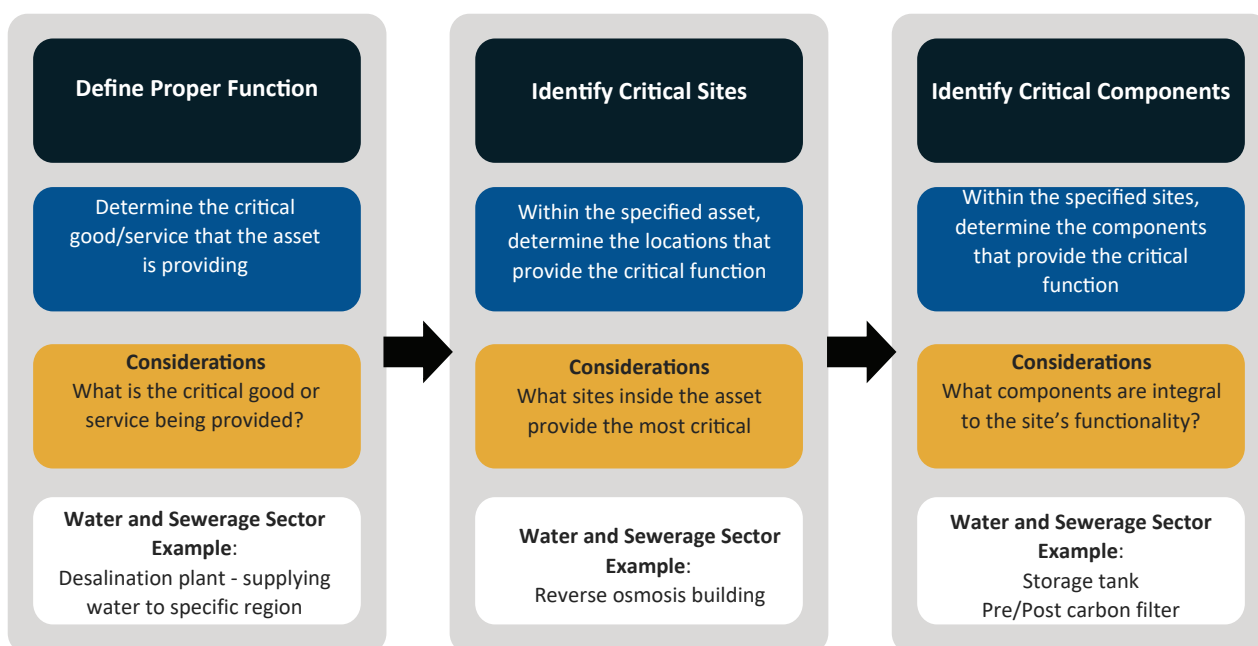
- (a) operating water or sewerage systems or networks; or
- (b) manufacturing or supplying goods, or providing services, for use in connection with the operation of water or sewerage systems or networks.

### Identifying and assessing criticality

For Water and Sewerage 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 Australian water provider has been identified as critical as it owns, manages and operates all water and sewerage services for a state or territory. The proper function of this asset is defined as being able to deliver drinking water and wastewater services 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.

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 those that could cause significant damage to the asset where they have been compromised, or are missing or damaged. For a water or sewerage organisation, critical components may include an automatic shut-off valve that stops the flow of water to the drain once the storage tank is full, or a dual media pressure filter that removes fine particles from seawater.



## 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 Water and Sewerage Sector:

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

### Emerging Trends

- **Climate change as a disrupter:** Has the potential to remake the ways in which water is naturally depleted and replenished, requiring organisations to adapt to these changes quickly.
- **Water is a contributor to Australia's image:** Supports image of a Australia as a clean, healthy and prosperous society, inviting immigration and tourism.
- **Increased agricultural production:** The world's population is expected to reach more than nine billion in 2050. The world requires more food to sustain this growth and the higher demand will challenge water resources and ecosystems.
- **Reusing wastewater:** The water cycle is traditionally linear. Discharged wastewater contains valuable resources such as nitrogen, phosphorous and energy that can be recovered and reused in a circular economy to preserve threatened resources.

### Emerging Technology

- **Enterprise and industrial control system convergence:** Leveraging technology to automate and remotely manage infrastructure and operations.
- **Developing new waste treatment methods:** To improve speed efficiency and quality within the waste treatment process to make better use of waste treatment by-products.
- **Developing better water treatment methods:** To make more out of wastewater, particularly in drought affected regions and, in irrigation and agriculture; this includes desalination and creating potable water for reuse. Better water treatment processes have also provided infrastructure builders the ability to avoid major wastewater infrastructure augmentations.
- **Developing advanced analytical tools:** Improving forecasting and supporting real-time decision making.
- **Asset augmentation:** Using technology for better monitoring of assets, particularly field service mobility, works management and remote inspection technologies such as drones, CCTV cameras and IOT sensors. Asset health and maintaining resilience of infrastructure is a key priority for water providers.
- **Intelligent asset management:** Leading water utilities have been building intelligence asset management into their processes. Implementation of other technologies has resulted in an every-increasing volume of information available. In this context, intelligence management integrates and organises all this data in order to make better decisions.
- **Artificial intelligence:** This helps to provide more sustainable management of water resources and automates that are costly to manage manually.
- **Using 5G to manage water service infrastructure:** 5G's low latency and ability to connect millions of devices in a small area will result in an increased capacity in autonomous infrastructure operations.



## 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 (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/>



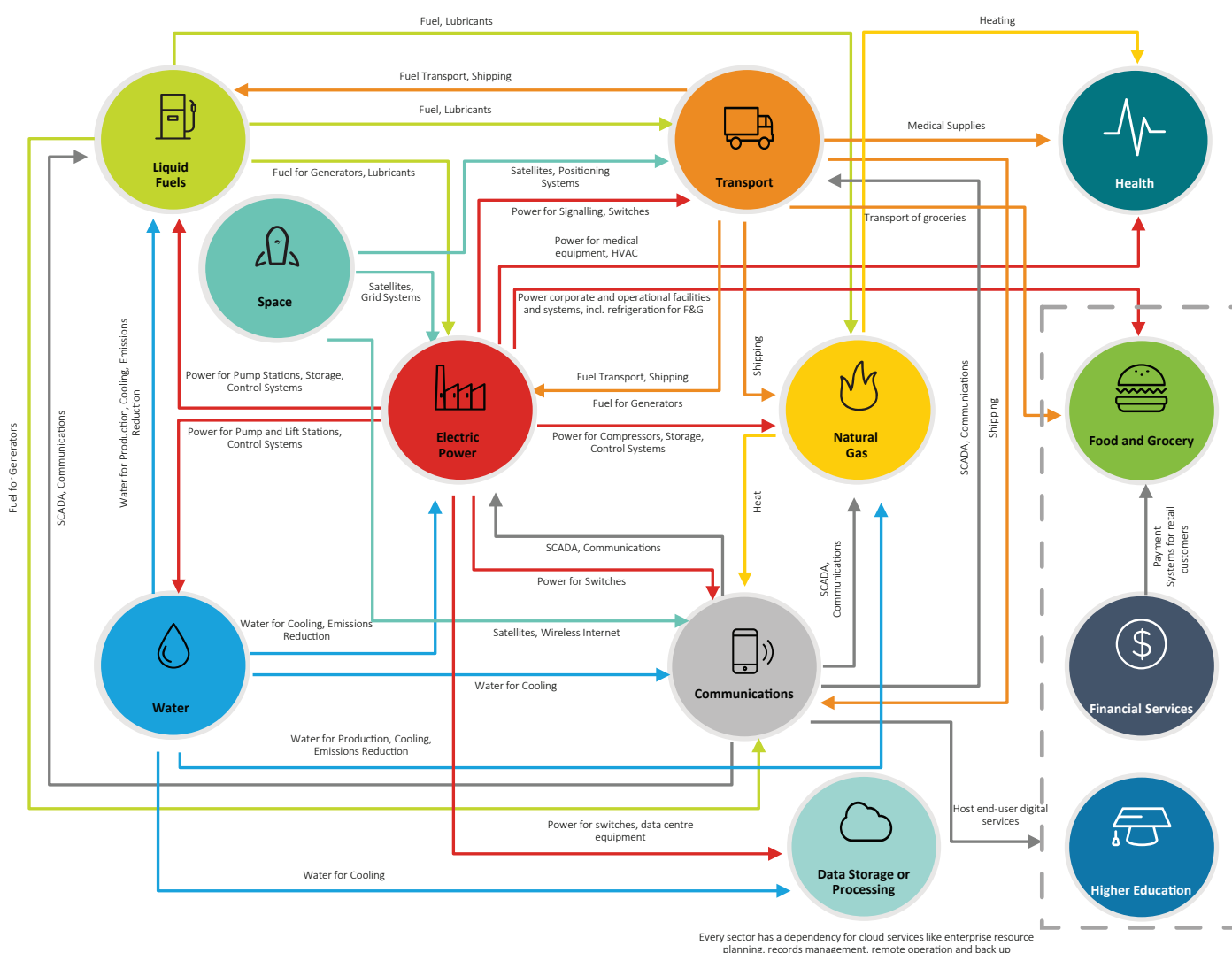
## Interdependencies (upstream and downstream)

### 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 Water and Sewerage 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.

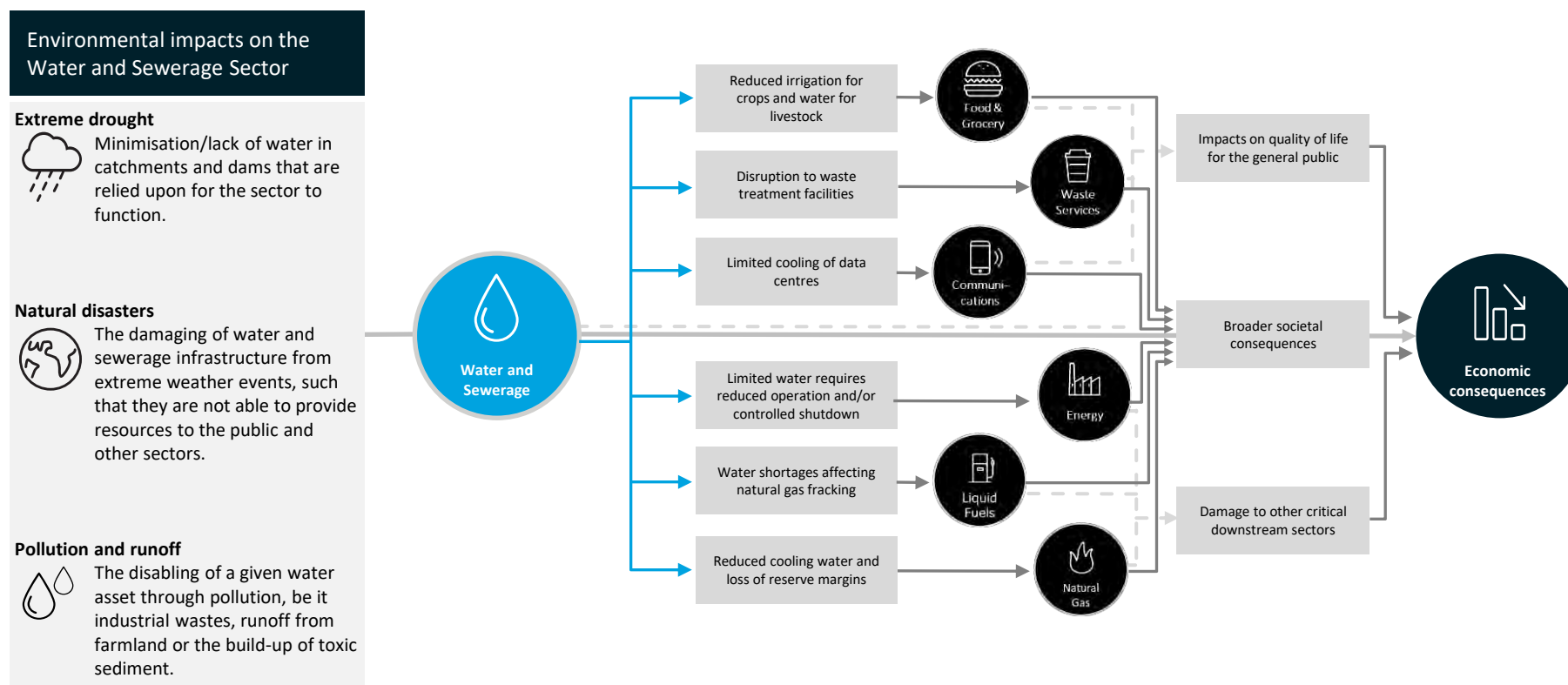
Figure 4. An example of sector interdependencies and relationships



## Flow-on effects for relevant impacts against Water and Sewerage 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 Water and Sewerage Sector.

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





An outage affecting a critical asset in the Water and Sewerage Sector could result in significant economic or societal implications. Impacts could vary based on factors including the geographic breadth of the outage, and the detriment of the impact to the broader water network. For example:

- In November 2019 a sewage pumping station discharged approximately 504,000 litres of raw sewage from a leaking sewer line, flowing into Orphan School Creek, NSW. The EPA issued AUD30,000 worth of fines to a water company for water pollution caused by this incident. The incident affected two unnamed creeks and, in this instance, the company is alleged to have failed to adequately clean up the overflow.
- In September 2015, the NSW EPA warned people living and working near RAAF Williamtown that elevated levels of toxic chemicals had been found in the surrounding area. Toxic chemicals used for firefighting that do not break down in the environment were found, affecting waterways and soil conditions in the area.
- Climate change and extreme weather events such as bushfires and floods can impact wastewater and clean water transport infrastructure. They can damage water infrastructure during an event, but also lead to lasting effects after the event, such as increases amounts of nutrients in waterways causing algal blooms and other hazards to drinking water supplies.
- Automation and centralisation of remote infrastructure management capabilities may increase efficiency, but has the potential, if compromised, to enable an attacker to access multiple parts of the water network, causing widespread disruption. A motivated attacker may also seek to make specific unauthorised changes to local environments, intentionally compromising water quality and perhaps contaminating the supply.
- From a legal and financial perspective, there is potential for significant consequences for an event in the Water and Sewerage Sector, from class action lawsuits relating to damage caused by water release, to fines or regulatory action relating to water quality or contamination, as well as action related to environmental damage from effluent release. A security-related attack has the potential to cause a wide variety of events that may result in legal or financial action against an organisation.

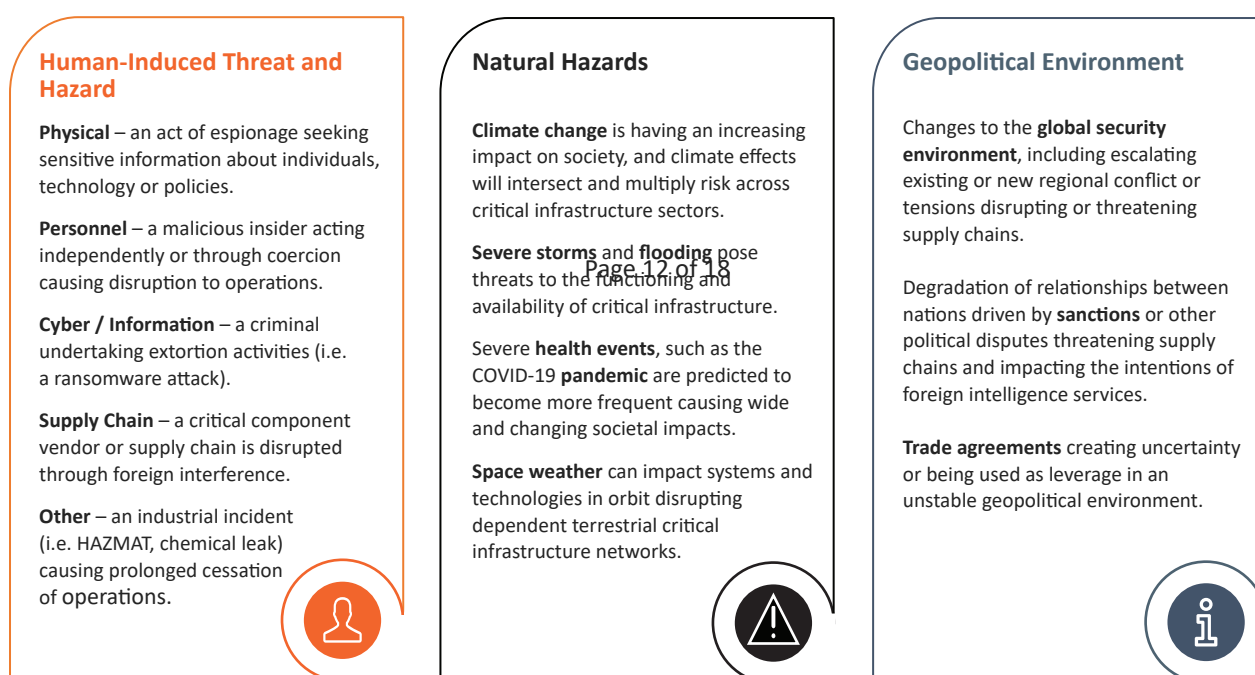


## Understanding threats and hazards for risk

### Identifying a threat and hazard landscape of the Water and Sewerage 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 Water and Sewerage Sector is an attractive target, and natural hazards can severely damage the infrastructure and the water 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, while the Water and Sewerage Sector – driven by improvements in technology and the need to meet commercial outcomes – will become more interconnected. This means that stakeholders in the Water and Sewerage Sector need to reevaluate risks regularly.

Natural hazards are becoming more frequent and intense; their impacts enduring and complex. The Water and Sewerage Sector is susceptible to such hazards through damage to facilities, componentry, and impacts to water quality.






## Understanding sector-specific risks

This table outlines a select example of identified threat and hazard vectors that impact Water and Sewerage 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"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Countries seeking to disrupt Australia's critical infrastructure may use advanced persistent threats or other modus operandi to scope, exert influence to disable water utilities and/or create disruption or cessation of water and sewerage services.
	Cyber-espionage	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Cyber espionage could be used to exfiltrate, monitor, intercept and manipulate data pertaining to water control systems and, current and future capabilities.
	Remote access to operational technology	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	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"> <li>Integrity</li> <li>Availability</li> </ul>	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"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> </ul>	Ransomware deployed into the networks of water providers has the potential to halt the functioning of an asset for extended periods with the intent to extract financial benefits.
 NATURAL	Severe weather events	<ul style="list-style-type: none"> <li>Integrity</li> <li>Availability</li> <li>Reliability</li> </ul>	Water infrastructure is likely to be impacted by more frequent extreme weather and natural disasters, causing damage or delay to the capability provided from the sector.
	Recurring environmental hazards	<ul style="list-style-type: none"> <li>Integrity</li> <li>Availability</li> <li>Reliability</li> </ul>	Recurring environmental hazards are threats that may be gradual in effect but have potential to affect infrastructure. Unless identified and treated, algal blooms and water quality events may damage the output of water infrastructure.

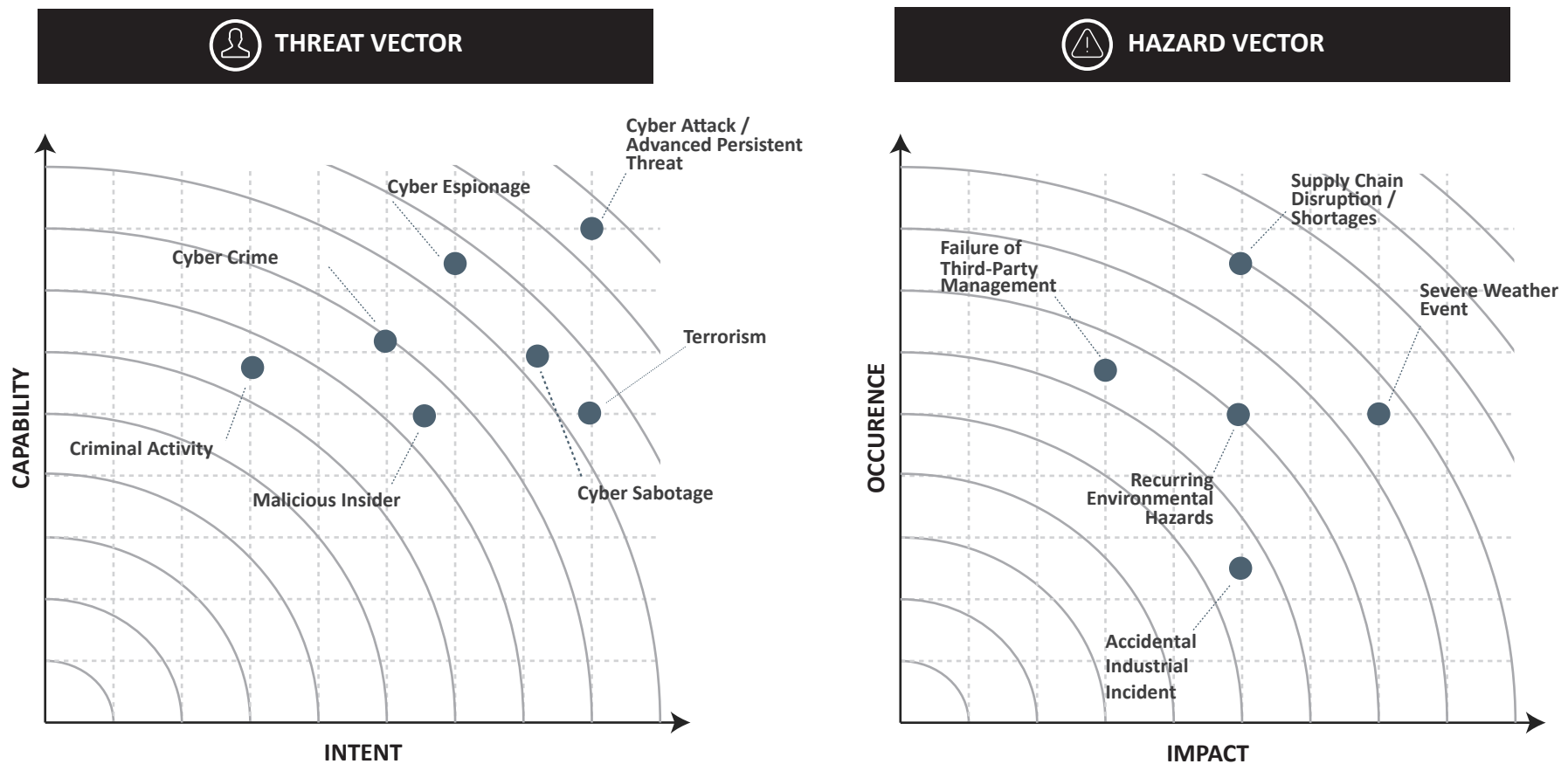


	Threat or Hazard Vector	Area of Potential Impact	Risk Scenario Considerations
 <b>PHYSICAL</b>	Criminal Activity	<ul style="list-style-type: none"> <li>Integrity</li> <li>Availability</li> <li>Reliability</li> </ul>	Criminal activity can damage Water and Sewerage Sector infrastructure through the illegal disposal of chemicals. This hazardous waste can erode and damage infrastructure, as well as cause issues with grey-water treatment.
	Terrorism	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Availability</li> <li>Reliability</li> </ul>	Groups that seek to make political statements through unlawful means may intentionally damage power plants, grids and wider networks to cause civil unrest.
 <b>SUPPLY CHAIN</b>	Supply issues/shortages	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Availability</li> <li>Reliability</li> </ul>	The reliance of the Water and Sewerage Sector upon third parties for water and waste treatment chemicals means the sector could be vulnerable to damage indirectly, through compromises to supply.
	Failure of third-party management	<ul style="list-style-type: none"> <li>Availability</li> <li>Reliability</li> </ul>	Failure by third parties to provide resources to the Water and Sewerage Sector have the potential to fail; consequent failure to provide resources disables the asset downstream.
	Foreign Interference in supply chain by extra-judicial actions	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Reliability</li> </ul>	Foreign powers seeking to exert influence on the Australian economy may conduct sabotage or espionage or undertake direct extra-judicial actions to damage the sector.
 <b>PERSONNEL</b>	Malicious Insider	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Integrity</li> <li>Availability</li> <li>Reliability</li> </ul>	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"> <li>Integrity</li> <li>Availability</li> <li>Reliability</li> </ul>	Hazards, such as an accidental industrial incident can cause significant risk for a entity. For the Water and Sewerage 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 Water and Sewerage 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

Water and Sewerage 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 Water and Sewerage 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.