



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

Reliant on defence industry and alliances – which requires a high level of security.

Increasing reliance on industrial control systems – and automated operational technology (OT) for equipment.

Susceptible to third-party attacks – particularly as integrity and confidentiality throughout the supply chain is critical to maintaining security.

National importance – both for the delivery of critical services such as telecommunications, weather monitoring, and global positioning systems, and for maintaining national security.

High availability requirements – particularly for signals and communication.

Growing reliance on cloud-based services – which increases the attack surface.

Potentially targeted by state actors – given the strategic and national security importance

High growth industry – as both governments and private corporations provide investment, the sector becomes more widely accessible.

Highly susceptible to natural hazards – including physical and environmental damage.



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 Space Technology Sector is framing a possible risk to a compromise of ground station infrastructure in order to collect on data transmitted or received, damaging the integrity of satellite communications.

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

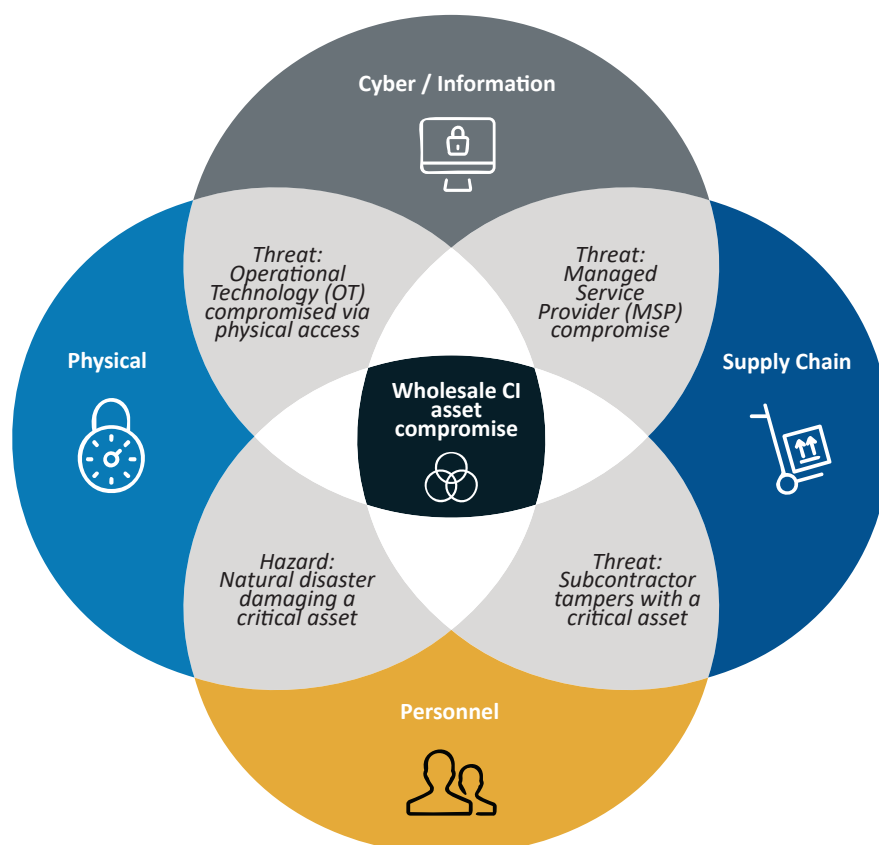
Some entities in the Space Technology Sector have security-related regulations already in place. Entities in the sector may need to consider guidance such as The Space (Launches and Returns) Act 2018 and its associated rules, or look to their state or territory government for regulatory frameworks and 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:

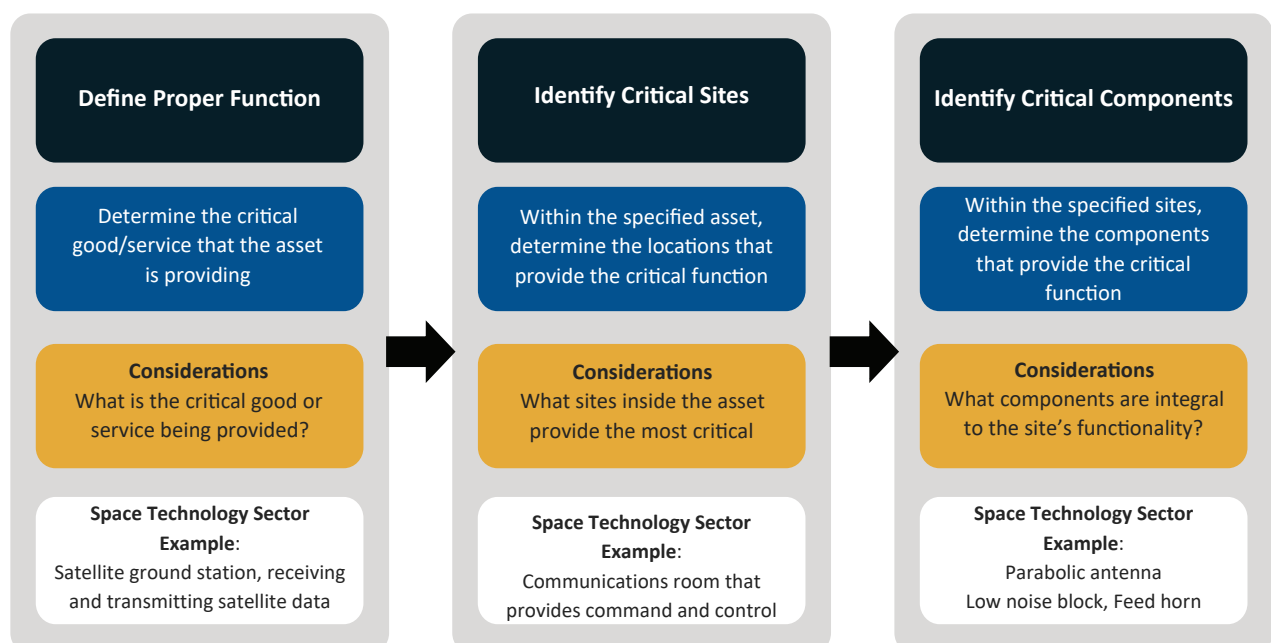
space technology sector means the sector of the Australian economy that involves the commercial provision of space-related services.

Identifying and assessing criticality

For Space Technology 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.

Within critical assets, critical sites are where the proper functions of these assets are located; these could include launch sites, control rooms, satellite assembly sites and data centres that host critical software. Critical sites are physical locations that are critical for an asset to achieve its proper function. 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 a space technology organisation, critical components may include tracking telemetry and command equipment used to receive and send satellite communications, or a feed horn used to gather reflected signals from the satellite dish and transfer them to a low noise block.



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 Space Technology Sector:

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

Emerging Trends

- **Foreign laws and changes in geopolitics altering the supply of space technology:** This is leading to more localized development and construction of space technology assets. While this may have the potential in reducing risks arising from geopolitical instability, conversely, it may increase supply chain risk, arising from material shortages or logistical challenges.
- **Changing regulatory landscape to facilitate commercial interest:** As more private organisations seek to deploy and manage assets, regulation will likely continue to be reactive, in part, due to the Space Technology Sector's relative infancy.
- **Improved standards for the quality of space-based assets:** Much of the current infrastructure in space today was built in a period where security was a lower priority, and the threat from cyber security was minimal. Furthermore, major security gaps remain in current satellite production as manufacturers tend to prioritise fast and cheap production over security.
- **Ground station security and data quality is critical to ongoing integrity:** This is a key target for disrupting service and signals between ground and space segments. Denial to, or poor quality of, data has flow on affects to the operations in multiple critical infrastructure sectors.

Emerging Technology

- **Potential disputes over electromagnetic (EM) spectrum allocation:** More assets are using similar communications frequencies leading to the need for greater management of EM 'pollution'.
- **Increased reliance on new capabilities emerging from technological advancement:** For example, in a positioning context, current technology typically allow for positioning within a 5–10 metre accuracy, but the Commonwealth of Australia is currently progressing a program that aims to improve accuracy to within 3cm in areas with mobile phone coverage and 10cm everywhere else. This will deliver more accurate, reliable and instantaneous positioning across Australia and its maritime zones.
- **Emerging capabilities for space:** Advancement in space technology is enabling developments like edge computing in space. Edge computing is an emerging paradigm aiding responsiveness, reliability and scalability of terrestrial computing and sensing networks, like cellular and Internet of Things (IOT). Frontier areas where Australia can lead and bolster the broader economy include constellations of miniaturized spacecraft for communications, earth observation and the IoT.



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/>



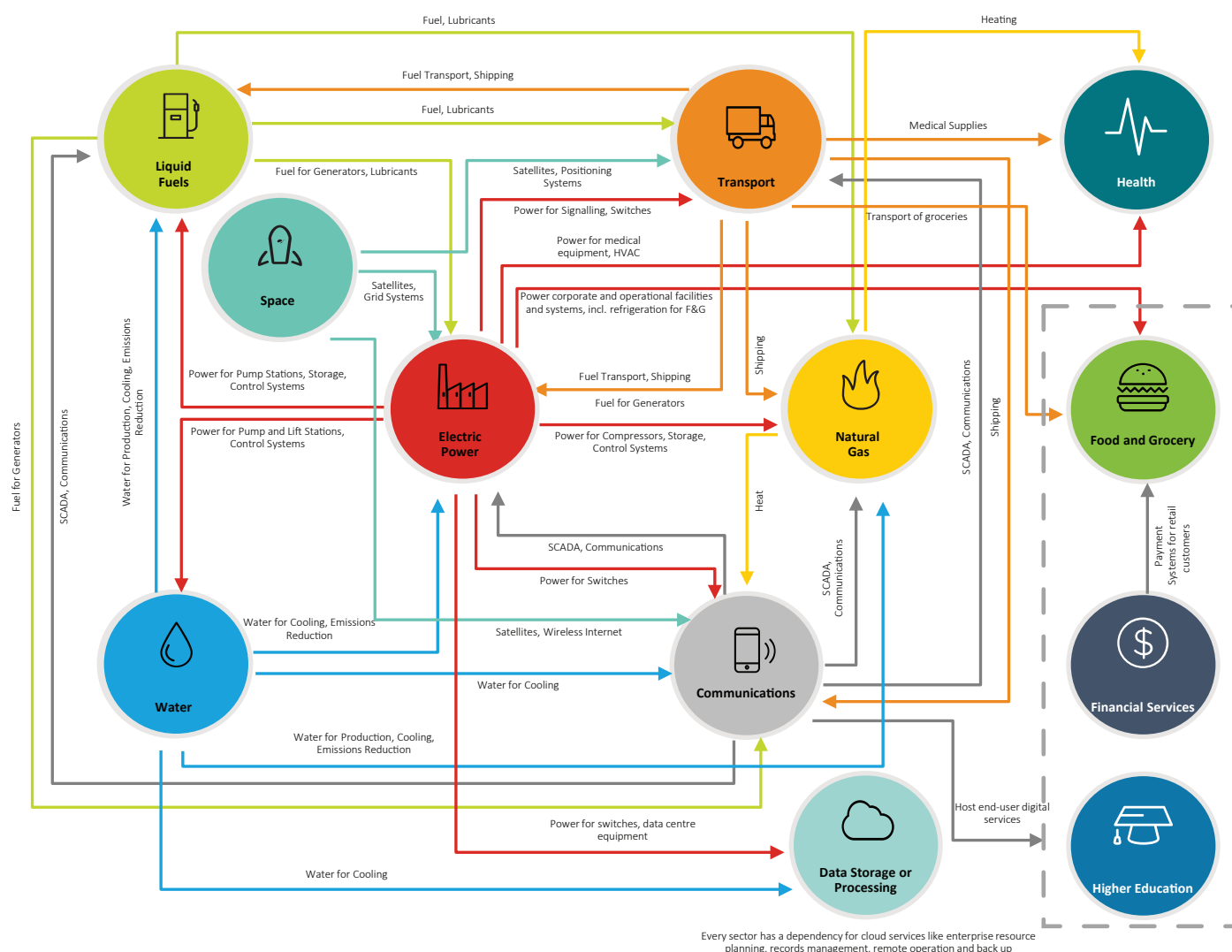
Interdependencies (upstream and downstream)

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 Space Technology 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.

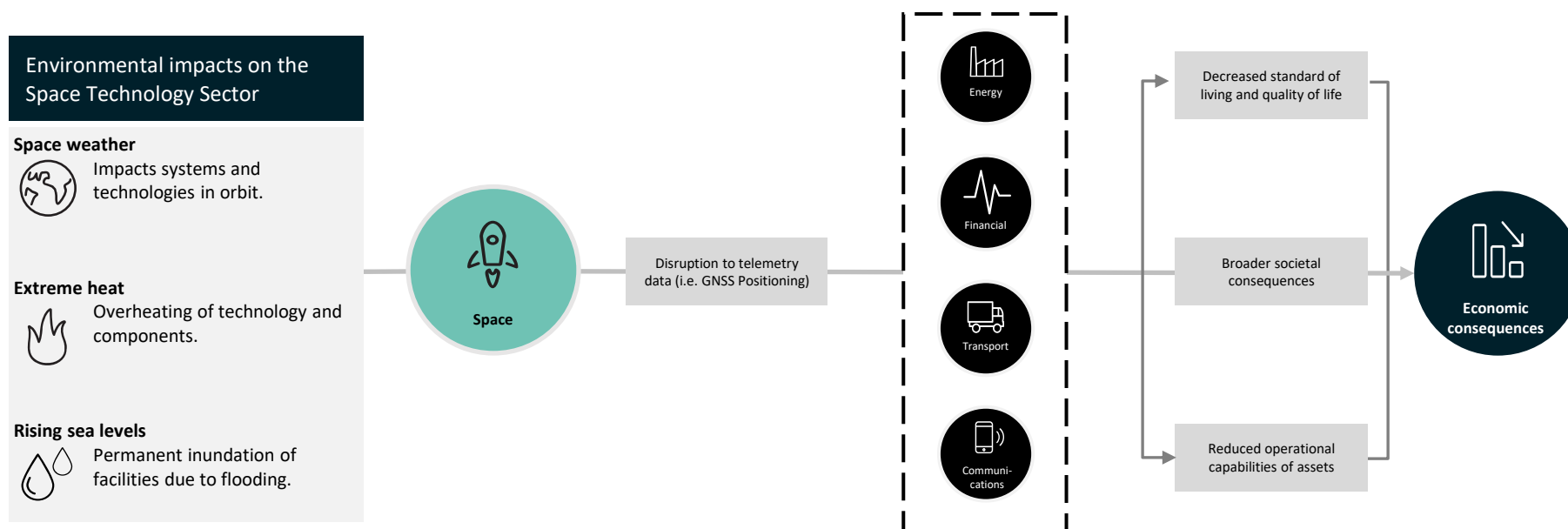
Figure 4. An example of sector interdependencies and relationships



Flow-on effects for relevant impacts against Space Technology 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 Space Technology Sector.

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





An outage affecting a critical asset in the Space Technology 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 space technology network. For example:

- Securing the supply chain is a critical function of the Space Technology Sector. In September 2020, it was discovered that a China-based data company had developed a database that had enabled Australia's space and science sectors to be tracked since 2019. The leaked database contained import–export data related to Australia's space program, attained through import–export agents, and revealed that confidential parts of Australia's space technology supply chain had been compromised.
- The financial impacts of interference with Space Technology Sector assets may include contract breach costs, as a result of service impacts to clients, and the replacement of expensive damaged equipment.
- Space communication is relied upon by a number of critical infrastructure assets in other sectors for services such as GNSS positioning data and for internet access in remote areas. Therefore, a disruption within the Space Technology Sector could impact the availability of assets in locations that have a high dependence on space-enabled services.

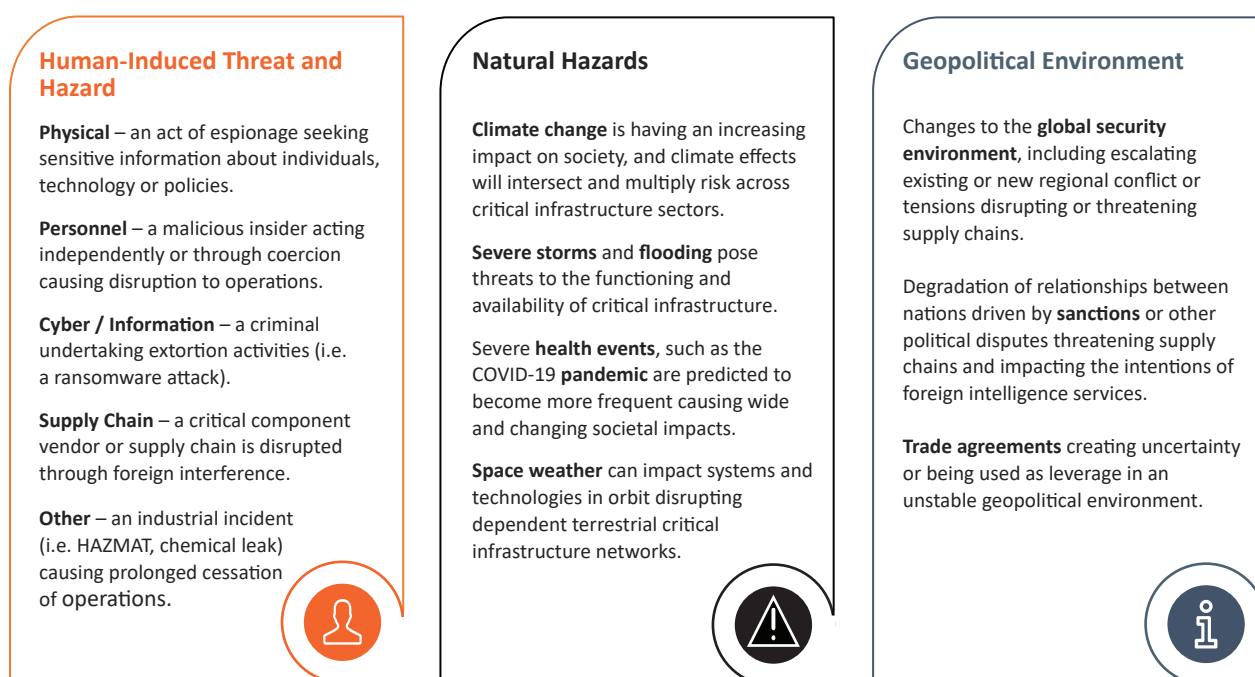


Understanding threats and hazards for risk

Identifying a threat and hazard landscape of the Space Technology Sector

All-hazards risk assessment considers both human-induced and natural threats and hazards. Given its role in critical infrastructure, the Space Technology Sector is an attractive target, natural hazards can severely damage the sector's infrastructure and space weather can damage extra-terrestrial assets. 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 Space Technology Sector, driven by improvements in technology and the need to meet commercial outcomes, will become more interconnected. This means that stakeholders in the Space Technology Sector need to reevaluate risks regularly.

Natural hazards are becoming more frequent and intense, their impacts enduring and complex. The Space Technology Sector is susceptible to these kinds of hazards through damage to facilities, and to componentry in orbit and on Earth.






Understanding sector-specific risks

This table outlines a select example of identified threat and hazard vectors that impact Space Technology 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 satellite networks to create disruption or cessation of communication and PNT services.
	Cyber-espionage	<ul style="list-style-type: none">ConfidentialityIntegrityAvailability	Cyber espionage could be used to exfiltrate, monitor, intercept and manipulate data pertaining to satellite networks 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 communication 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">AvailabilityReliability	Satellite infrastructure is likely to be impacted by more frequent extreme weather and natural disasters, causing damage to critical communication network equipment.
	Space weather event	<ul style="list-style-type: none">ConfidentialityAvailabilityReliability	Coronal mass ejections from space weather events threaten to disable space technology through interplanetary magnetic fields. Additionally, critical infrastructure can be disabled through damage caused to general and GPS satellites in orbit.

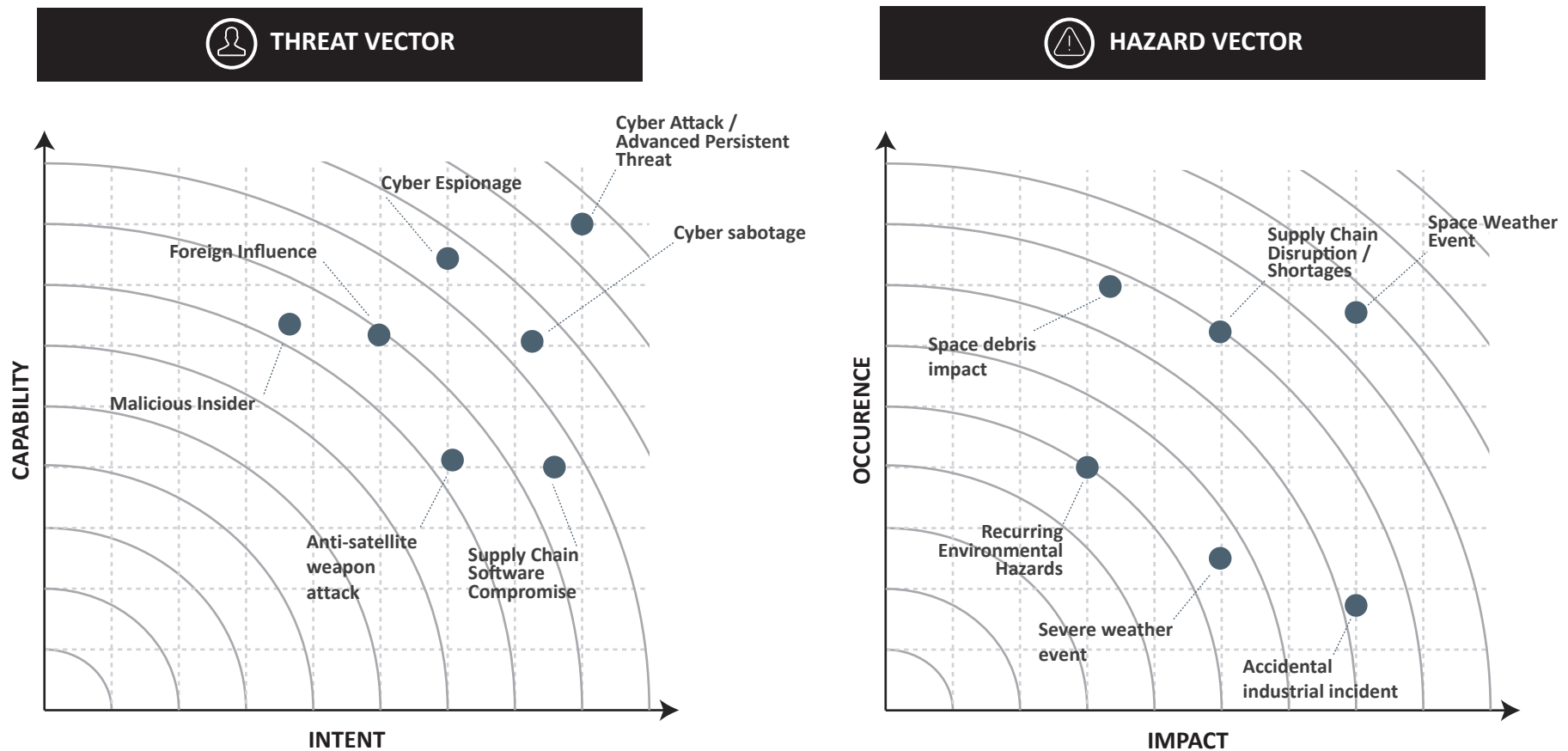


	Threat or Hazard Vector	Area of Potential Impact	Risk Scenario Considerations
 PHYSICAL	Anthropogenic space hazards	<ul style="list-style-type: none"> Integrity Availability Reliability 	Space debris and pollution pose a risk of damaging spacecraft and satellites in orbit. Major damage could affect the functioning of the asset and compromise its availability, integrity and reliability to transmit data.
	Proliferation of Anti-Satellite (ASAT) weapons	<ul style="list-style-type: none"> Integrity Availability Reliability 	The threat of hostile behaviour in space is likely to increase, with active development and testing of direct-ascent and co-orbital ASAT weapons, both kinetic and non-kinetic, heightening the risk to military and non-military satellite assets.
 SUPPLY CHAIN	Supply issues/shortages	<ul style="list-style-type: none"> Confidentiality Availability Reliability 	The sector relies on internationally-sourced specialised components and advanced technologies; shortages of these will directly affect the functioning of communication assets.
	Compromised / faulty componentry in satellite supply chain	<ul style="list-style-type: none"> Confidentiality Availability Integrity Reliability 	The sector relies upon foreign businesses for critical satellite componentry. This can cause issues for space assets if imported components are poor quality or contain intentional vulnerabilities to be used as backdoors.
	Foreign Interference in supply chain by extra-judicial actions	<ul style="list-style-type: none"> Confidentiality Integrity Reliability 	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"> 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 technology used by assets with the intent to cause harm.
	Accidental industrial incident	<ul style="list-style-type: none"> Integrity Availability Reliability 	Hazards, such as an accidental industrial incident can cause significant risk for a entity. For the Space Technology Sector, an incident causing damage to launch infrastructure may result in the destruction of rockets and payloads.

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 Space Technology 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:

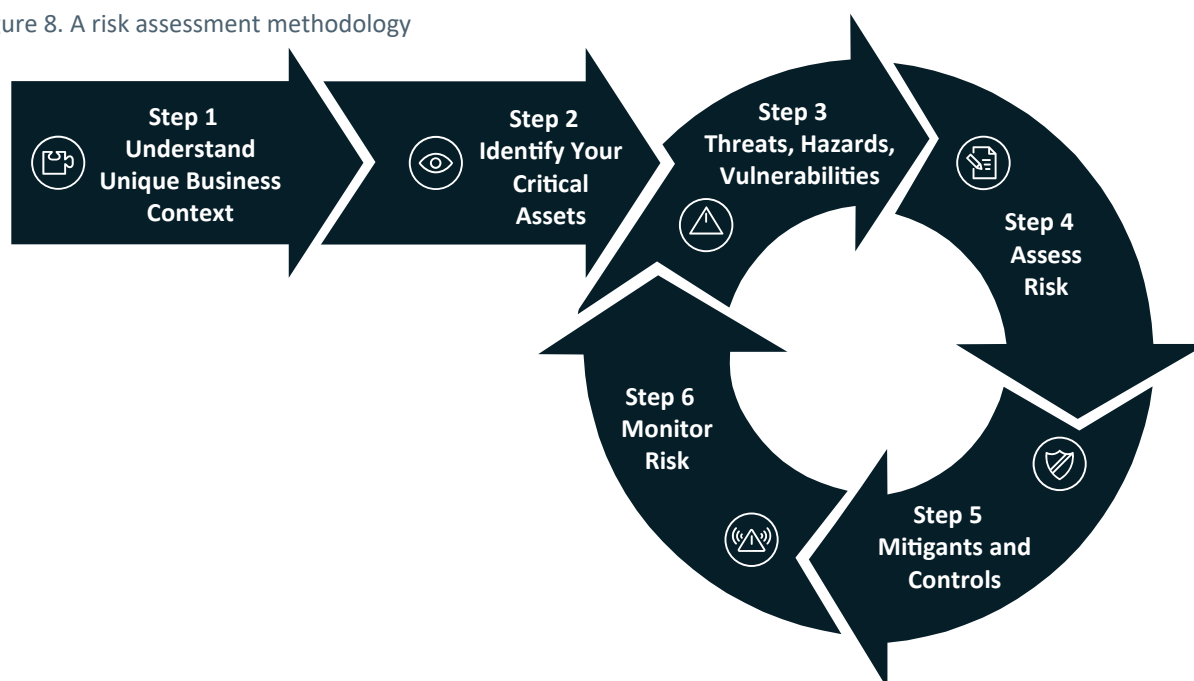
- Ease of implementation
- Cost-effectiveness
- Whether the action creates new risks and/or unintended consequences
- Environmental impacts (positive and negative)
- Multi-objective actions
- Long-term and short-term results
- Effectiveness
- Direct and indirect benefits
- Legal, regulatory, social and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



Appendix – A risk assessment methodology

Space Technology 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 Space Technology 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.