Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Risk Assessment Advisory for Critical Infrastructure

Higher Education and Research 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 Higher Education and Research 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 **Higher Education and Research Sector** are outlined below:

Multi-user networks – university intranet, Eduroam, and AARNET connections.

Reliance on external funding – government funding, student fees and external donations.

Internationally recognised – and highly respected for innovation and the quality of education programs.

Significant government investment – into research and development.

Large amounts of sensitive data – classified or dual-use research as well as student and staff information.

Collaboration with domestic defence agencies and industry – including involvement in classified research projects and education.

Leading-edge research – including the sensitive and potentially controversial areas of robotics, artificial intelligence, medicine, biology, quantum computing, and military research.

Culture of openness and sharing – which promotes learning and collaboration both domestically and internation.

Decentralised and fragmented – making consistency in security practices a challenge.

Increasing cloud adoption – including proliferation of methods to deliver learning remotely.

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 Higher Education and Research Sector is framing a possible risk to the provision of learning resources for universities, affecting the higher education of students in a specialised field of study and/or the ability to conduct critical research.

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 Higher Education and Research Sector has been provided in the **Understanding sector-specific risks** section of this document.

Some entities in the Higher Education and Research Sector have security-related regulations already in place. Entities in the sector may need to consider guidance such as the Tertiary Education Quality and Standards Agency Act 2011 (TEQSA Act) or the University Foreign Interference Taskforce (UFIT) Guidelines to Counter Foreign Interference, 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.

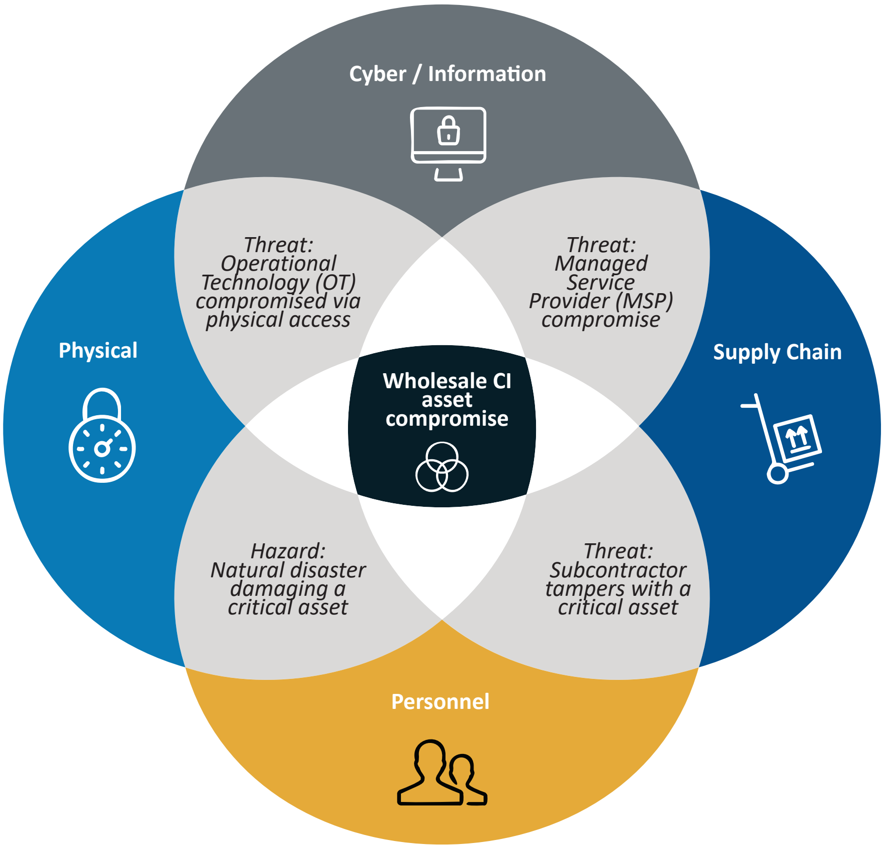
Entities should also refer to other CISC sector guidance for further information.

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


Cyber / Information
Physical
Supply Chain
Personnel
Threat: Operational Technology (OT) compromised via physical access
Threat: Managed Service Provider (MSP) compromise
Wholesale CI asset compromise
Hazard: Natural disaster damaging a critical asset
Threat: Subcontractor tampers with a critical asset

Determining criticality of assets

Security of Critical Infrastructure Act 2018 (SOCI Act) – Section 5:

Higher education and research sector means the sector of the Australian economy that involves undertaking a program of research that is

(a) supported financially (in whole or in part) by the Commonwealth; and

(b) critical to:

(i) a critical infrastructure sector (other than the higher education and research sector); or

(ii) national security; or

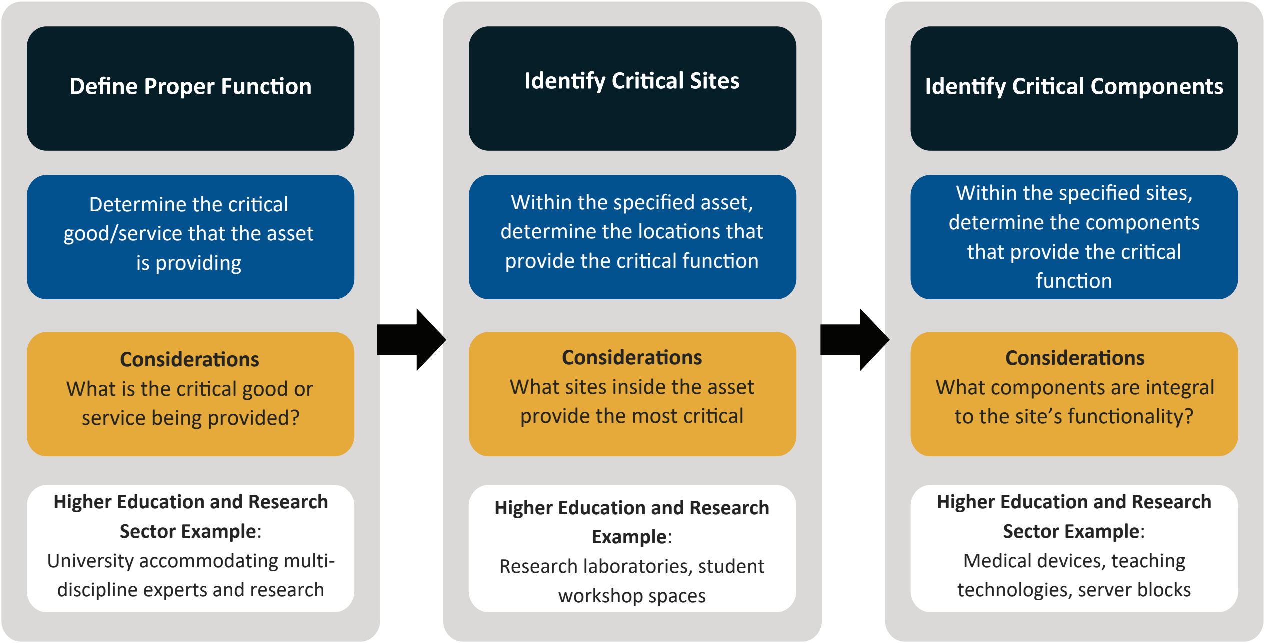
(iii) the defence of Australia.

Identifying and assessing criticality

For Higher Education and Research 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


Define Proper Function
Determine the critical good/service that the asset is providing
Considerations
What is the critical good or service being provided?
Higher Education and Research Sector Example:
University accommodating multi-discipline experts and research
Identify Critical Sites
Within the specified asset, determine the locations that provide the critical function
Considerations
What sites inside the asset provide the most critical
Higher Education and Research Example:
Research laboratories, student workshop spaces
Identify Critical Components
Within the specified sites, determine the components that provide the critical function
Considerations
What components are integral to the site's functionality?
Higher Education and Research Sector Example:
Medical devices, teaching technologies, server blocks

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

Critical sites are physical locations that are part of an asset that are required for it to maintain its proper function. For a hospital, this could include intensive care units or maternity wards, and could also include data centres that host ICT services.

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 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 research organisation, critical components may include laboratory equipment or systems used for learning. Damage to, or disablement of, these systems may prevent the research process, endanger the asset, and impact the progress of the studied technology.

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 Higher Education and Research Sector:

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

Emerging Trends

- **Adaptive learning:** Recent advances in technology mean the education industry has been able to better adapt to the needs of students. This is an overall positive result as it means more effective learning for students, as well as reduced wasted resources for education providers.
- **eLearning platforms:** These provide the functionality required for developing and managing an online course along with peer communication and effective interaction, aimed at increasing student engagement.
- **Gamification:** Along with simulation, is a trend that refers to the incorporation of game elements into the learning process, which improve learning approaches not only in educational institutions but in business environments as well (i.e. during recruitment).
- **Smart displays:** In recent years the sector has seen an increase in interactive displays to teach and communicate. Initially with larger devices, such as smart boards, this trend has now scaled down to iPads ad similar interactive devices.

Emerging Technology

- **Education technologies based on AI:** Cutting edge technology has seen the emergence of AI applications in the education sector. The use of this technology could potentially make processes within the sector more effective and efficient.
- **Augmented reality and simulations:** These have left a mark in the world of visuals. Today, its impact has started to control the way students learn and collaborate with their teachers.
- **Usage of 5G technologies in education:** Through enhancements of 5G, students are able to benefit from increased resource accessibility. This will take the form of quick downloads of student files and resources via more powerful networks.
- **Automation:** Education as a whole can be streamlined through automation, for instance, lectures can be digitally scheduled and tracked.
- **Learning analytics:** As an emerging technology, learning analytics is a broad process that utlises activity tracking and analysis. This technology is now being used by teachers to better record the learning behaviours of students.

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.

ACSC Australian Cyber Security Centre

Australian Cyber Security Centre (ACSC)
A hub for private and public sector collaboration and information sharing on cyber security. to preventand combat threats and minimise harm to Australians.

ASIO

Australian Security Intelligence Organisation (ASIO) Outreach
Provides advice to government, industry and academia on current and emerging security threats.

For further information on TISN and how to join the network, please go to: *https://www.cisc.gov.au/engagement/trusted-information-sharing-network*

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*

To register to the Outreach program and gain access to security updates, please go to: *https://www.outreach.asio.gov.au/*

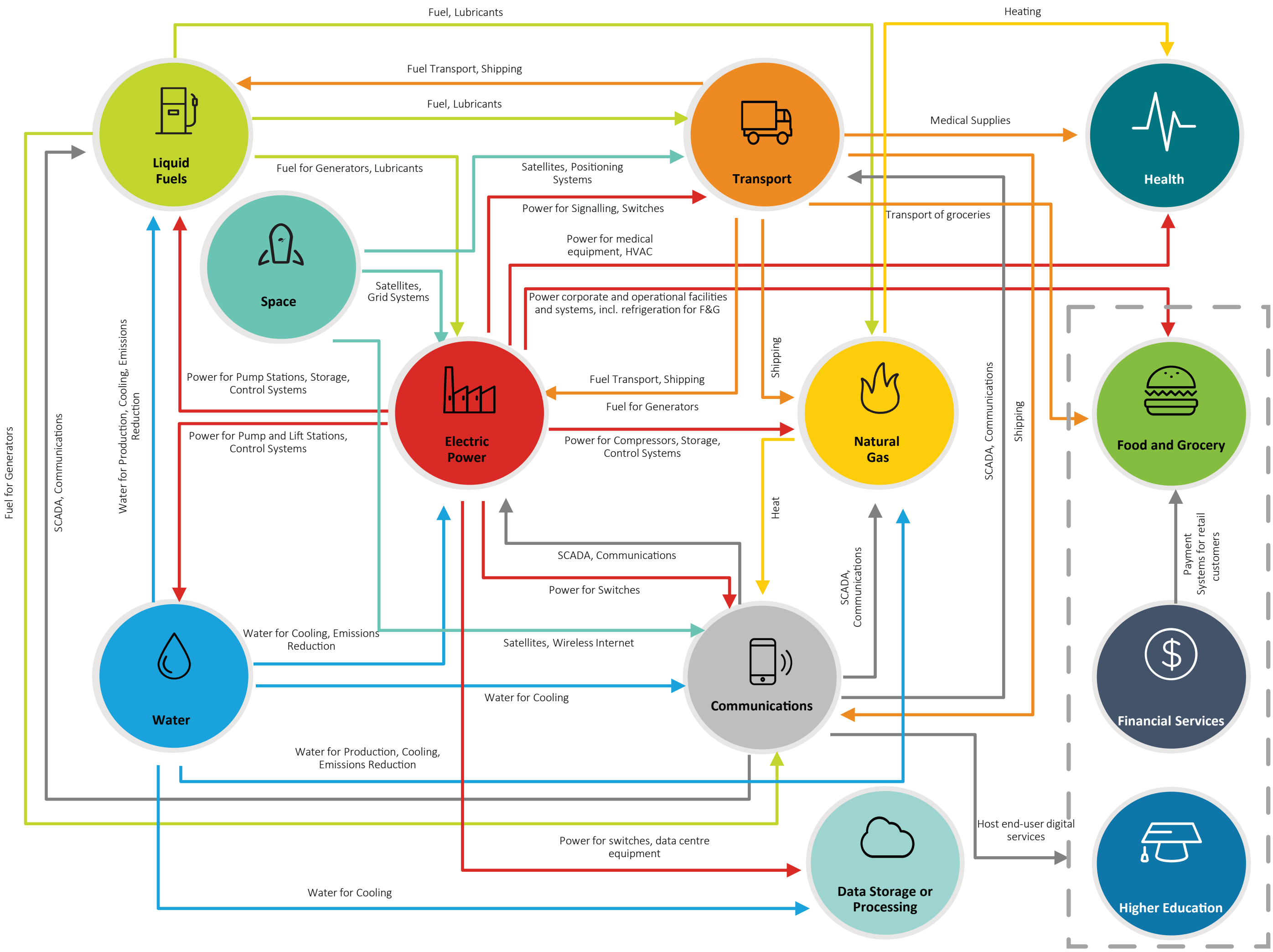
Interdependencies (upstream and downstream)

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 Higher Education and Research 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

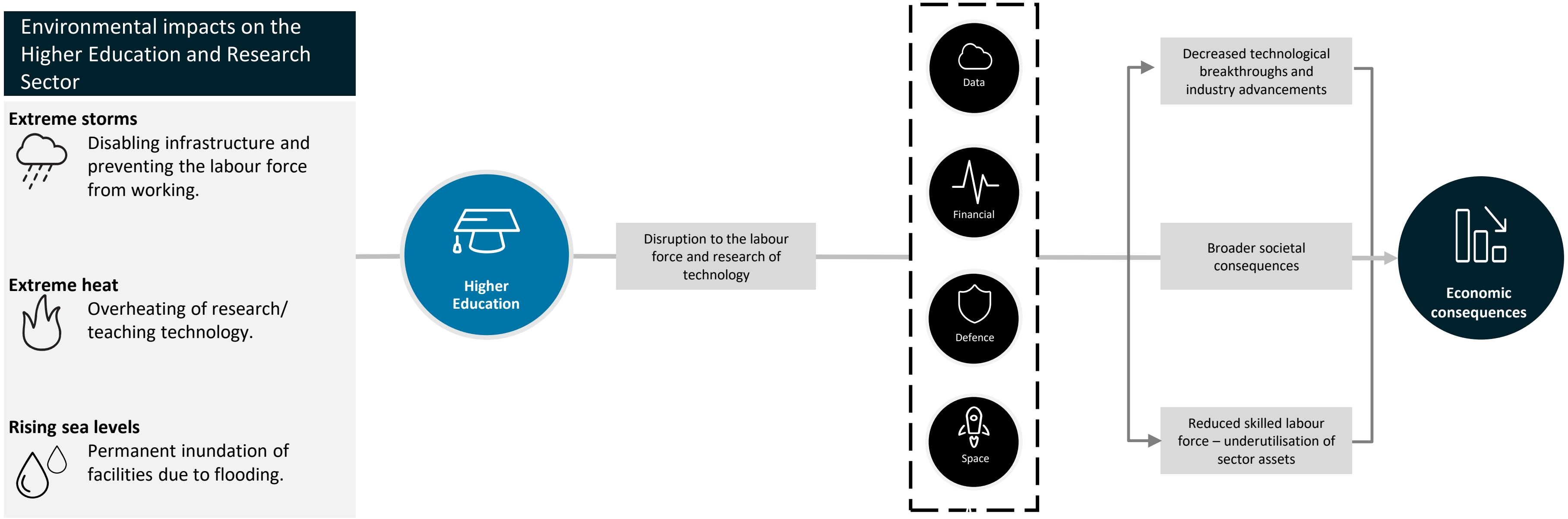

Fuel, Lubricants
Heating
Fuel Transport, Shipping
Fuel, Lubricants
Medical Supplies
Liquid Fuels
Transport
Health
Fuel for Generators, Lubricants
Satellites, Positioning Systems
Power for Signalling, Switches
Transport of groceries
Space
Power for medical equipment, HVAC
Satellites, Grid Systems
Power corporate and operational facilities and systems, incl. refrigeration for F&G
Shipping
SCADA, Communications
Shipping
Fuel for Generators
SCADA, Communications
Water for Production, Cooling, Emissions Reduction
Power for Pump Stations, Storage, Control Systems
Fuel Transport, Shipping
Fuel for Generators
Power for Pump and Lift Stations, Control Systems
Power for Compressors, Storage, Control Systems
Electric Power
Natural Gas
Food and Grocery
Heat
SCADA, Communications
Payment Systems for retail customers
SCADA, Communications
Power for Switches
Water for Cooling, Emissions Reduction
Satellites, Wireless Internet
Water
Water for Cooling
Communications
Financial Services
Water for Production, Cooling, Emissions Reduction
Host end-user digital services
Power for switches, data centre equipment
Water for Cooling
Data Storage or Processing
Higher Education

Every sector has a dependency for cloud services like enterprise resource planning, records management, remote operation and back up

Flow-on effects for relevant impacts against Higher Education and Research 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 Higher Education and Research Sector.

Figure 5. Example of flow-on effects from an impact against the Higher Education and Research Sector



Environmental impacts on the Higher Education and Research Sector

Extreme storms
Disabling infrastructure and preventing the labour force from working.

Extreme heat
Overheating of research/ teaching technology.

Rising sea levels
Permanent inundation of facilities due to flooding.

Higher Education
Disruption to the labour force and research of technology
Data
Financial
Defence
Space
Decreased technological breakthroughs and industry advancements
Broader societal consequences
Reduced skilled labour force – underutilisation of sector assets
Economic consequences

An outage affecting a critical asset in the Higher Education and Research Sector could have significant economic or societal implications, varying depending on factors such as the geographic breadth of the outage and the impact on the broader research and education network. For example:

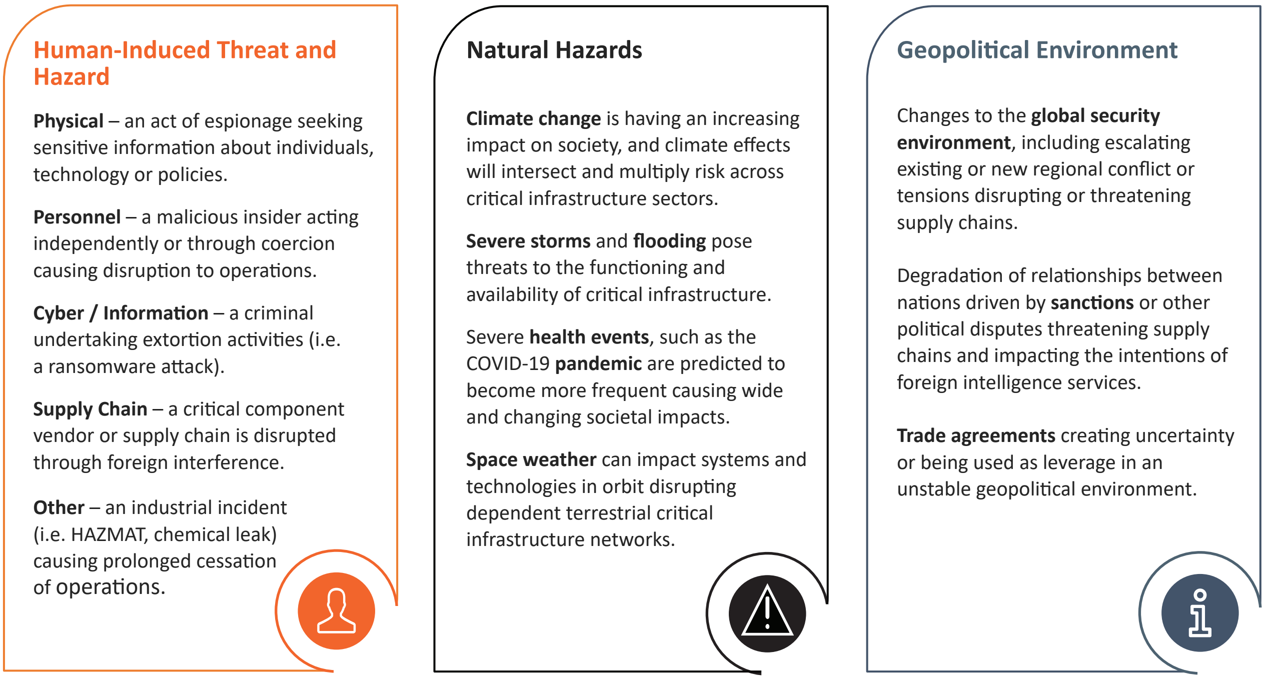
- A compromise in the security of university networks can lead to a leak of sensitive information such as research details, personal student and staff information, and details of defence projects. This can cause major damage to a university's reputation and reduce confidence for collaboration and investment.
- Pre-COVID-19, the international education was a significant and growing source of Australia's revenue, producing workers for domestic industry and providing training in critical areas. As a result, damage or disruption to the education sector may have wide-reaching implications for the Australian economy.
- Medical research, particularly in sensitive fields such as stem-cell research, viral research and genetic engineering, has the potential to cause significant reputational impacts if compromised or not reported appropriately. In addition, a compromise of information relating to human tissue, specimens or cadavers could result in legal or privacy action.
- Military and defence research may rely on information that is sensitive or classified within the Australian Government and which, if compromised, could provide a strategic advantage for Australia's adversaries. Additionally, a compromise of information sensitive to military organisations, such as the Defence Force Academy, could jeopardise the safety of Australian defence personnel.
- Upstream, the Higher Education and Research Sector is susceptible to geopolitical dynamics that may restrict international student immigration, as seen during the COVID-19 pandemic. Downstream, a reduced reputation of Australian universities could impact the number of international students and by extension, negatively affect sectors that rely on immigration and tourism.

Understanding threats and hazards for risk

Identifying a threat and hazard landscape of the Higher Education and Research Sector

All-hazards risk assessment considers both human-induced and natural threats and hazards. Given its role in critical infrastructure, the Higher Education and Research Sector is an attractive target for threat actors seeking societal disruption; and natural hazards can severely damage infrastructure and, supply of critical equipment and medicine. 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



Human-Induced Threat and Hazard

Physical – an act of espionage seeking sensitive information about individuals, technology or policies.

Personnel – a malicious insider acting independently or through coercion causing disruption to operations.

Cyber / Information – a criminal undertaking extortion activities (i.e. a ransomware attack).

Supply Chain – a critical component vendor or supply chain is disrupted through foreign interference.

Other – an industrial incident (i.e. HAZMAT, chemical leak) causing prolonged cessation of operations.

Natural Hazards

Climate change is having an increasing impact on society, and climate effects will intersect and multiply risk across critical infrastructure sectors.

Severe storms and **flooding** pose threats to the functioning and availability of critical infrastructure.

Severe **health events**, such as the COVID-19 **pandemic** are predicted to become more frequent causing wide and changing societal impacts.

Space weather can impact systems and technologies in orbit disrupting dependent terrestrial critical infrastructure networks.

Geopolitical Environment

Changes to the **global security environment**, including escalating existing or new regional conflict or tensions disrupting or threatening supply chains.

Degradation of relationships between nations driven by **sanctions** or other political disputes threatening supply chains and impacting the intentions of foreign intelligence services.

Trade agreements creating uncertainty or being used as leverage in an unstable geopolitical environment.

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 Higher Education and Research Sector, driven by improvements in technology and the need to meet commercial outcomes, will become more interconnected. This means that stakeholders in the Higher Education and Research Sector need to revaluate risks regularly.

Natural hazards are becoming more frequent and intense; their impacts enduring and complex. The Higher Education and Research Sector is susceptible to these kinds of hazards through damage to research facilities, learning environments, and to sensitive teaching/research technology.

Understanding sector-specific risks

This table outlines a select example of identified threat and hazard vectors that impact Higher Education and Research 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.

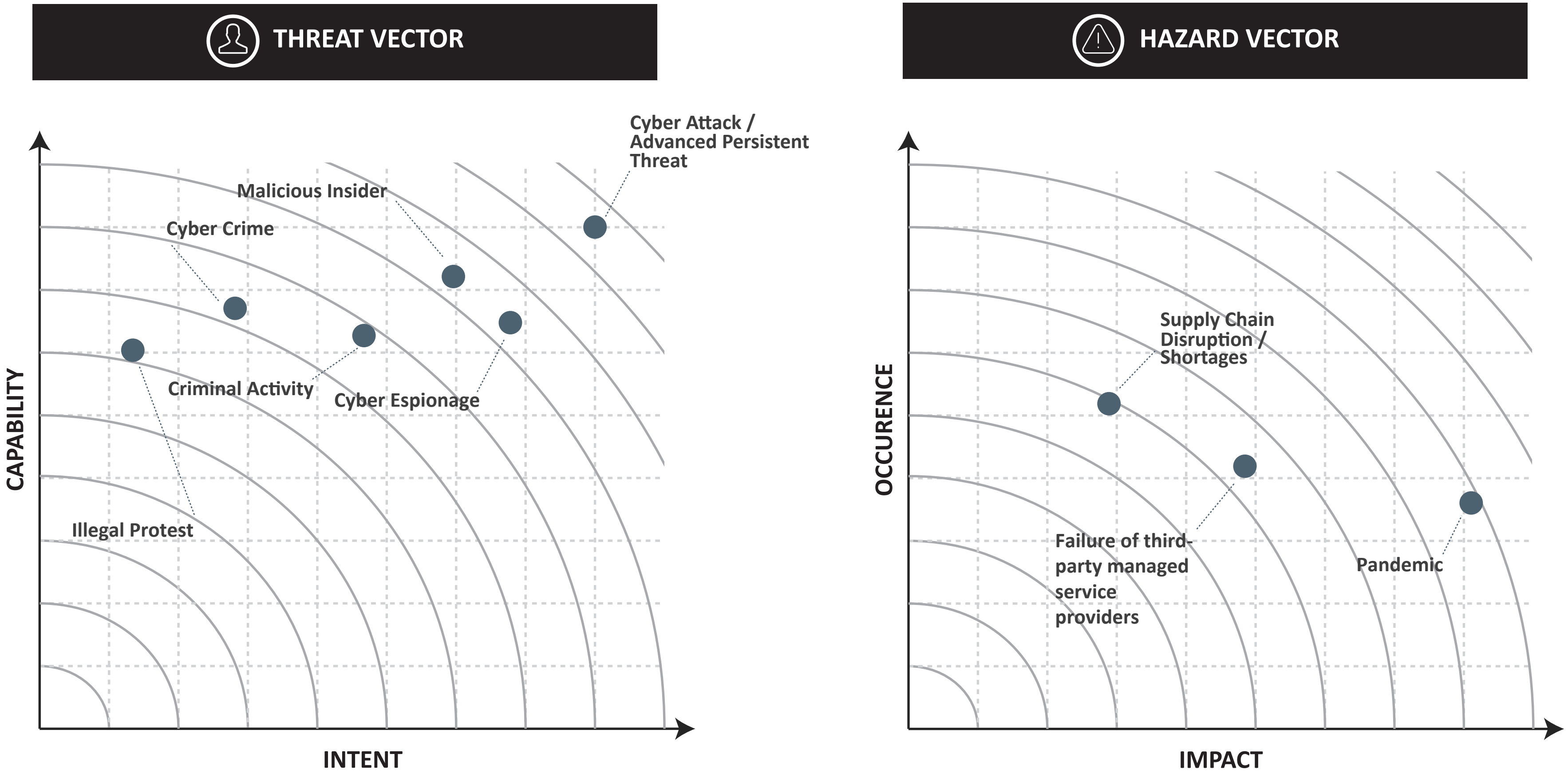
	Threat or Hazard Vector		Risk Scenario Considerations
CYBER / INFORMATION	Foreign interference	• Confidentiality • Integrity • Availability	Countries seeking to disrupt Australia's critical infrastructure may use advanced persistent threats or other modus operandi to scope to exert influence over research or access to technologies.
	Cyber-espionage	• Confidentiality • Integrity • Availability	Cyber espionage could be used to exfiltrate, monitor, intercept and manipulate data pertaining to sensitive, commercial or other research material.
	Financially-motivated cyber-crime	• Confidentiality • Integrity • Availability	Ransomware deployed into the networks of higher education and research providers has the potential to halt the functioning of an asset for extended periods with the intent to extract financial benefits.
NATURAL	Pandemic	• Confidentiality • Availability • Reliability	Pandemics such as COVID-19 have the potential to greatly alter the functioning of society, increasing the need for remote learning and collaboration, at times over less-than-secure conferencing platforms. Border and other travel restrictions also has indirect impacts on research and finances
PHYSICAL	Criminal activity	• 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.
	Illegal Protest	• Confidentiality • Availability • Reliability	Groups that seek to make political statements through unlawful means may intentionally damage university or research buildings and other infrastructure.

	Threat or Hazard Vector	Area of Potential Impact	Risk Scenario Considerations
SUPPLY CHAIN	Supply issues/shortages	• Confidentiality • Availability • Reliability	The reliance of the sector upon international supply lines and resources can have a significant impact through labour shortage or shortcomings in critical supplies.
	Failure of third-party managed service providers	• Availability • Integrity • Reliability	Third-party service providers relied upon to provide resources to the sector have the potential to fail, whether through management issues, capability shortcomings, or inadequate security practices.
PERSONNEL	Malicious Insider	• 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 Higher Education and Research Sector, malicious insiders may seek monetary gain by providing commercially-sensitive research to third party actors.

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 Higher Education and Research 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.

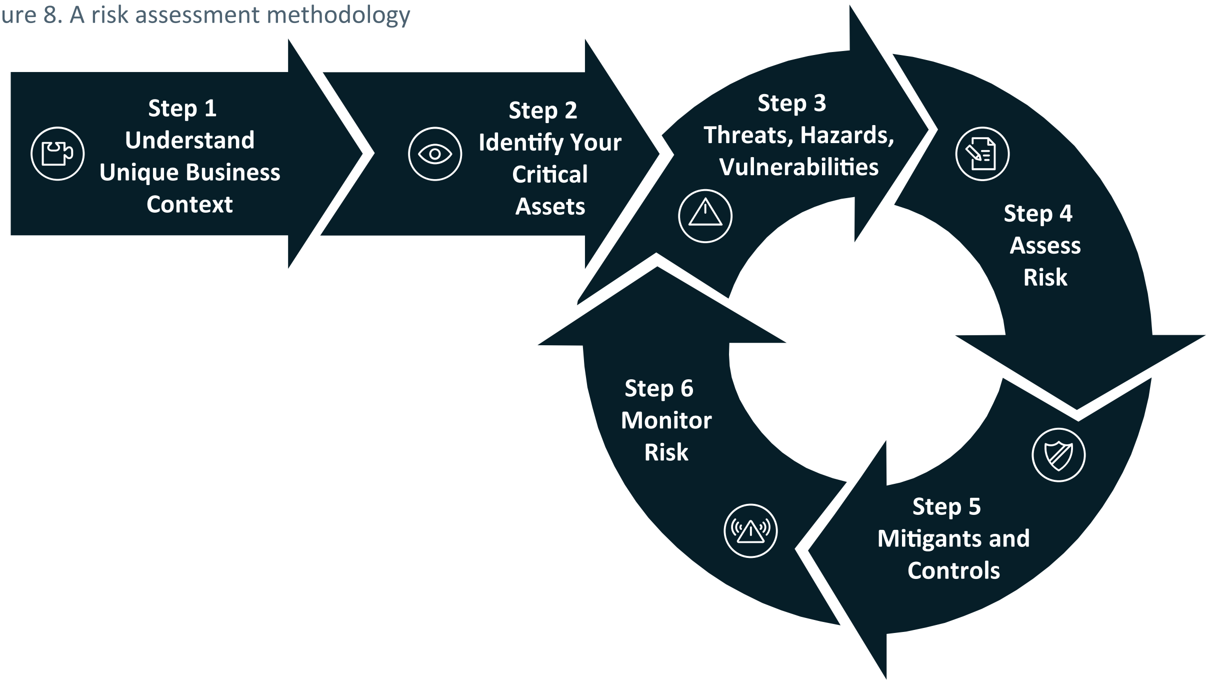
Once controls and mitigations options have been identified by an entity, these should be continually evaluated and prioritised, particularly as threats and vectors evolve. The following criteria can be used for development of an implementation plan for risk controls and mitigations:

- 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

Higher Education and Research 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 Unique Business Context
Step 2
Identify Your Critical Assets
Step 3
Threats, Hazards, Vulnerabilities
Step 4
Assess Risk
Step 5
Mitigants and Controls
Step 6
Monitor Risk

STEP 1 – Understand business and sector landscape and how it fits under critical infrastructure

Identify the context of your individual organisation within both the Higher Education and Research 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.