



## Risk Assessment Advisory for Critical Infrastructure

### Financial Services and Markets 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 Financial Services and Markets 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 **Financial Services and Markets Sector** are outlined below:

**An essential service** – without which the Australian economy is unable to function.

**High quantities of sensitive data** – the value of financial data makes the sector an attractive target for a range of threat actors.

**A primary target for financial crimes** – including fraud, identity theft, and money laundering.

**Highly regulated federally** – regulation and compliance are typically part of the culture of the sector.

**Incidents and outages can be extremely disruptive** – particularly in areas where banking and financial transactions are unavailable.

**Small players grow quickly** – proliferation of new ways of conducting business, such as cryptocurrency or buy-now-pay-later services.

**Largely siloed operators** – while playing a bridging role in finance and inter-bank/institution transactions, more holistic systemic and infrastructure-based cooperation within the sector is very limited.

**Early adopter of new technologies** – particularly in areas with tangible impacts to the financial sector, such as blockchain and automation.

**Significant use of third- and fourth-party relationships** – integration across multiple business processes.

**Embracer of digital platforms for innovation** – digitisation of banking platforms, use of cloud services, single-touch payment systems, and insurance claims applications.

**High concentration risk** – concentrated market with large players that have a significant market share.

The information contained in this document is general in nature and does not constitute legal advice. Readers are encouraged to obtain legal advice that applies to their particular circumstances. The Commonwealth of Australia does not guarantee the accuracy, currency or completeness of any information in this document.



## Risk in the critical infrastructure context

### Identifying risk for critical infrastructure

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

An example of how to identify this risk for the Financial Services and Markets Sector is framing a possible risk from a widespread disruption to the availability of payment systems, as to how it may cause significant disruption across multiple sectors (such as transport, food and grocery, telecommunications), thereby exacerbating and spreading the impact.

### 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 Financial Services and Markets Sector has been provided in the **Understanding sector-specific risks** section of this document.

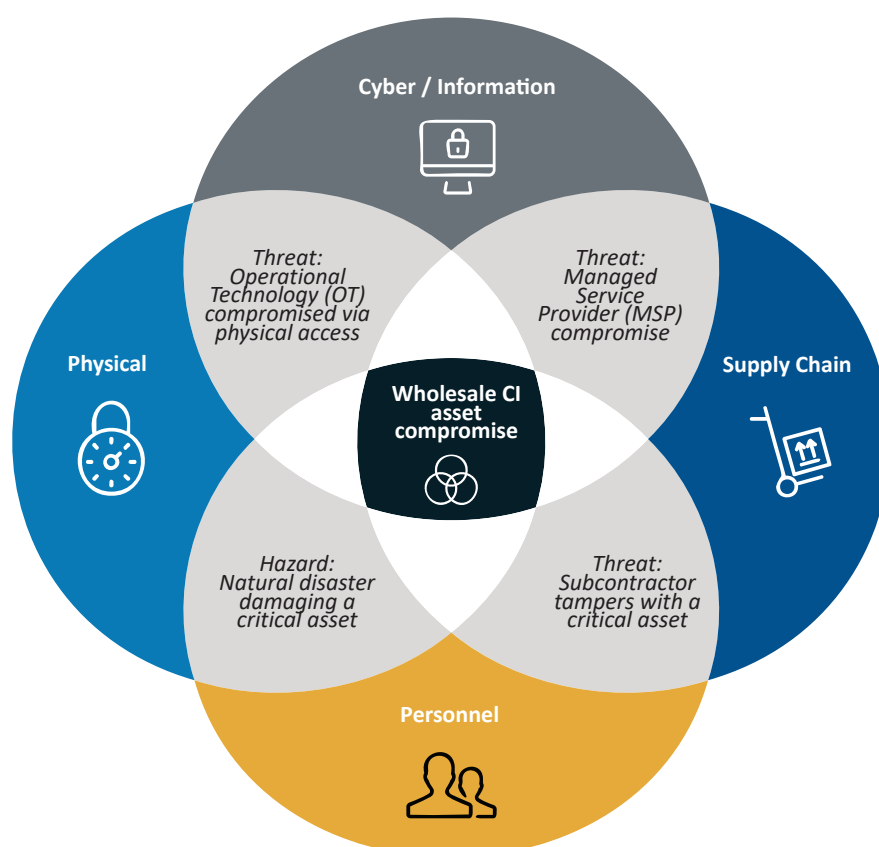
Some entities in the Financial Services and Markets Sector have security-related regulations already in place. Entities in the sector may need to consider guidance such as from the Australian Prudential Regulation Authority (APRA) and consider how they can incorporate national security-related risk into 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:*

financial services and markets sector means the sector of the Australian economy that involves:

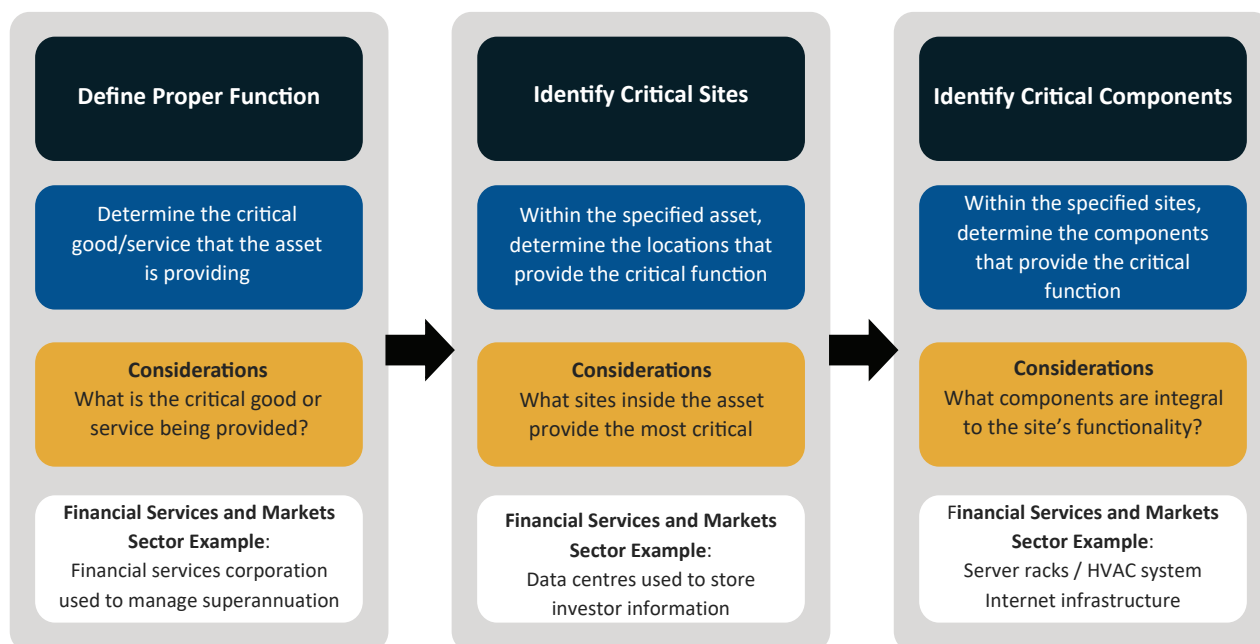
- (a) carrying on banking business; or
- (b) operating a superannuation fund; or
- (c) carrying on insurance business; or
- (d) carrying on life insurance business; or
- (e) carrying on health insurance business; or
- (f) operating a financial market; or
- (g) operating a clearing and settlement facility; or
- (h) operating a derivative trade repository; or
- (i) administering a financial benchmark; or
- (j) operating a payment system; or
- (k) carrying on financial services business; or
- (l) carrying on credit facility business.

### **Identifying and assessing criticality**

For Financial Services and Markets 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 bank has been identified as critical as it is fundamental to the Australian economy. The proper function of this asset is defined as being able to help customers manage their finances.

Critical sites are physical locations that are part of an asset required for it to maintain its proper function. This could include server rooms, sensitive financial instrument monitoring centres or other areas based on the context of the specific asset. Large financial assets like superannuation companies are networked assets that require a number of different sites and components to achieve their critical function.

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

Critical components are anything that is required to maintain the function of the asset, or whose absence, compromise or damage could cause significant harm to the asset. For a financial organisation, critical components may include things like servers and network infrastructure, but also HVAC systems, backup generators and physical access control devices.



## 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 Financial Services and Markets Sector:

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

### Emerging Trends

- **Financial Technology (FinTech) as a whole:** Since the rise of the internet, FinTech solutions such as AI, cloud, blockchain and big data have transformed the sector as a whole. This trend is most likely here to stay, with cutting edge solutions being the way of the future.
- **Mobile banking:** A rising trend in banking from personal devices has meant the sector has had to adapt and accommodate consumers that are used to being able to manage their lives from mobile devices.
- **Environmental, social and governance (ESG) reporting:** Like many other sectors, the Financial Services and Markets Sector has seen a rise in the use of ESG reporting. These reports outline an organisation's environmental, social and governance impact. This is in line with an increase in overall awareness of social and environmental justice across society.
- **Consumer data rights:** Growing data rights in other jurisdictions such as the European Union, and recent efforts to amend the Australian Privacy Act, may impact Financial Services and Markets Sector asset operations.

### Emerging Technology

- **Artificial Intelligence and chatbots:** Making effective use of large quantities of data that the finance industry is tasked with dealing with on a daily basis.
- **Robotic Process Automation (RPA):** Financial algorithms are an emerging feature of the industry through which data is processed and uploaded across applications and servers used by business.
- **Cloud computing:** Offloading of business processing to cloud services means that 24/7 banking services are available to customers, meaning data generation is increased.
- **Hyper-personalisation:** Services in the Financial Services and Markets Sector means that customers feel more valued and appreciated. Moreover, personalized services are more accurate and provide better results to consumers, saving time and resources.
- **Instant payments:** Due to the rise in personal devices with access to the internet, there is an increased demand for 24/7 rapid money transfers.
- **Blockchain:** This technology has the potential to upend business processes across the sector as a whole, though efforts, such as those by some large firms, to counter its decentralised nature, could limit its take up.



## 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/>

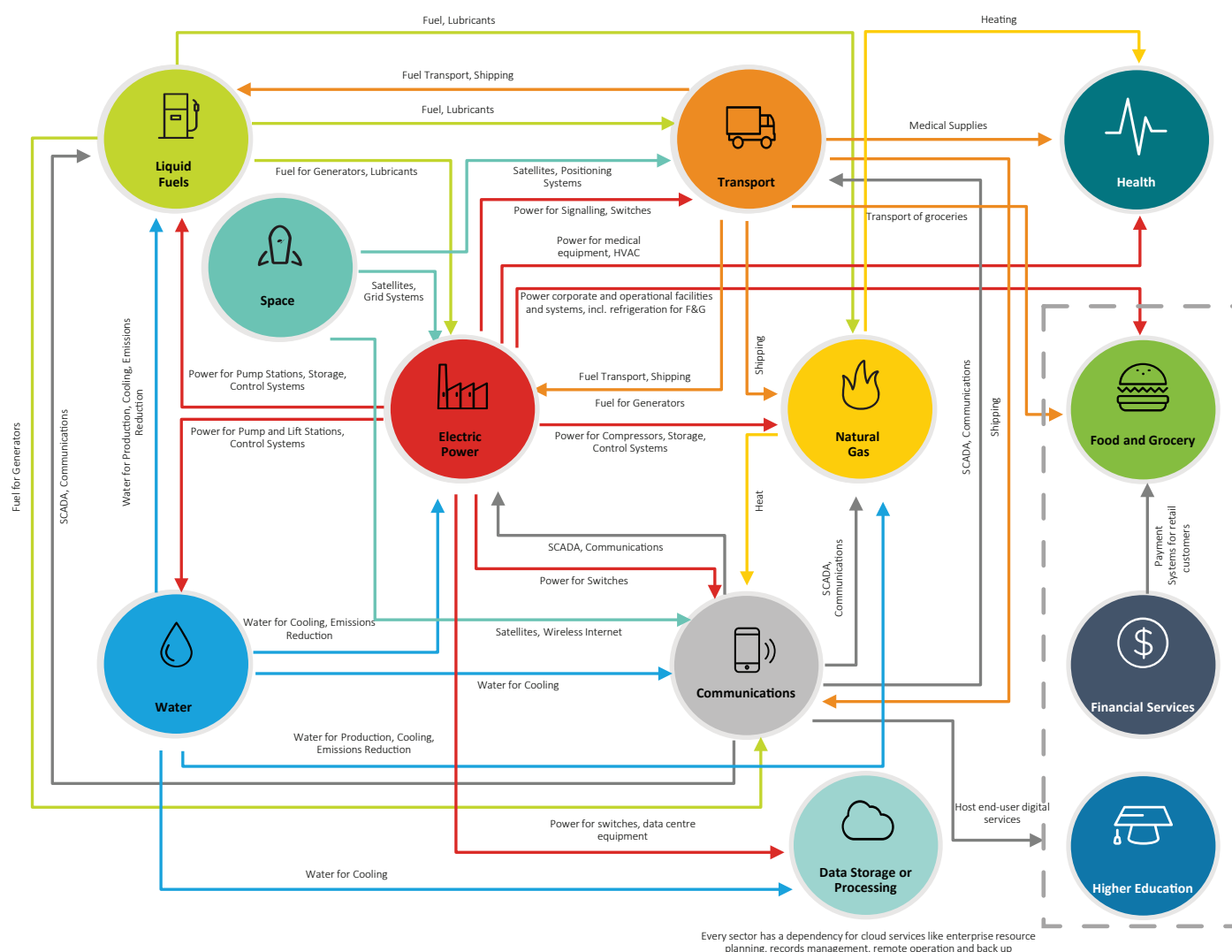
## Interdependencies (upstream and downstream)

### 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 Financial Services and Markets 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

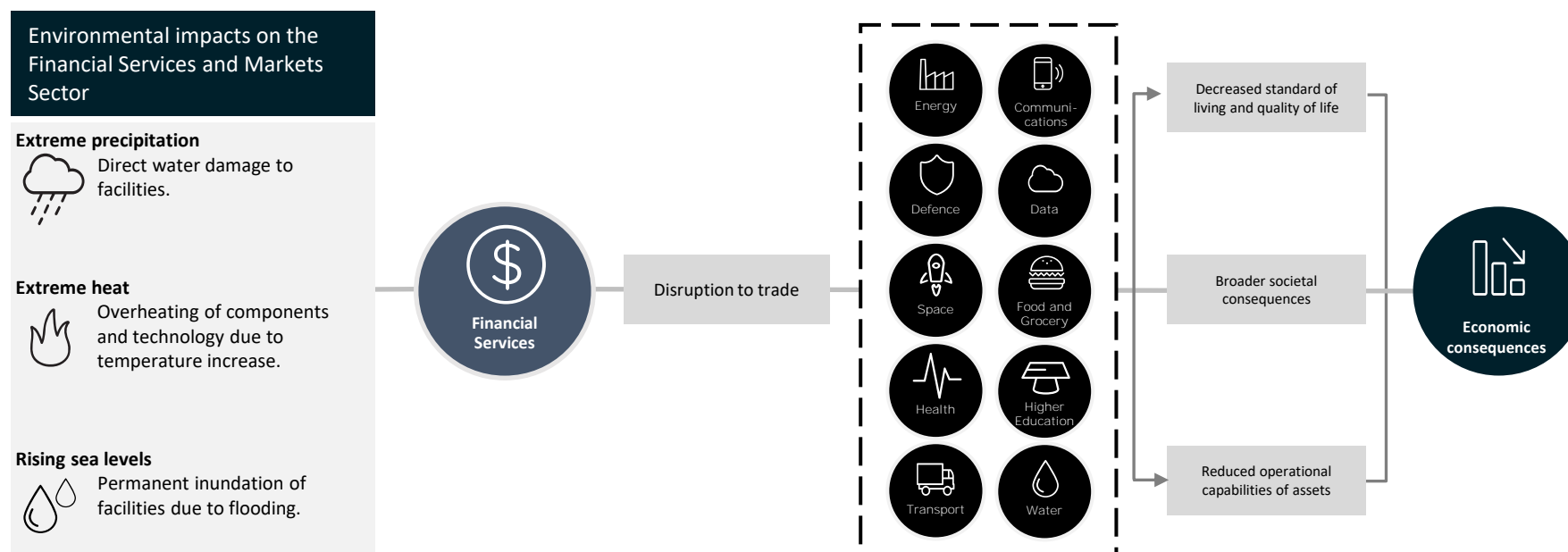




## Flow-on effects for relevant impacts against Financial Services and Markets Sector assets

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 Financial Services and Markets Sector.

Figure 5. Example of flow-on effects from an impact against the Financial Services and Markets Sector





An outage affecting a critical asset in the Financial Services and Markets Sector could result in significant economic or societal implications. Impacts could vary based on factors including the geographic breadth of the outage, and the number of companies in the sector affected. For example:

- In 2017, a consumer credit reporting agency experienced a large-scale data breach, with the data of an estimated 147 million people being compromised and exposed to identity theft. It is believed that this breach was caused by the compromise of a third-party software system used by the firm.
- Due to the distributed nature of the finance sector, extreme weather events have minimal impact on the sector as a whole, due to the reliance on cloud and off-premises data storage/processing. While this is true for the most part, situations still exist where weather events can simultaneously disrupt multiple separate critical sites or a system that is not cloud based.
- The economic damages from failing payment systems have worsened over the past five years due to the COVID-19 pandemic and the related reduction in the use of cash and physical currency. Citizens are thus less likely to be readily able to use cash during issues with financial institutions, as statistics indicate fewer people carry cash than they did five years ago.

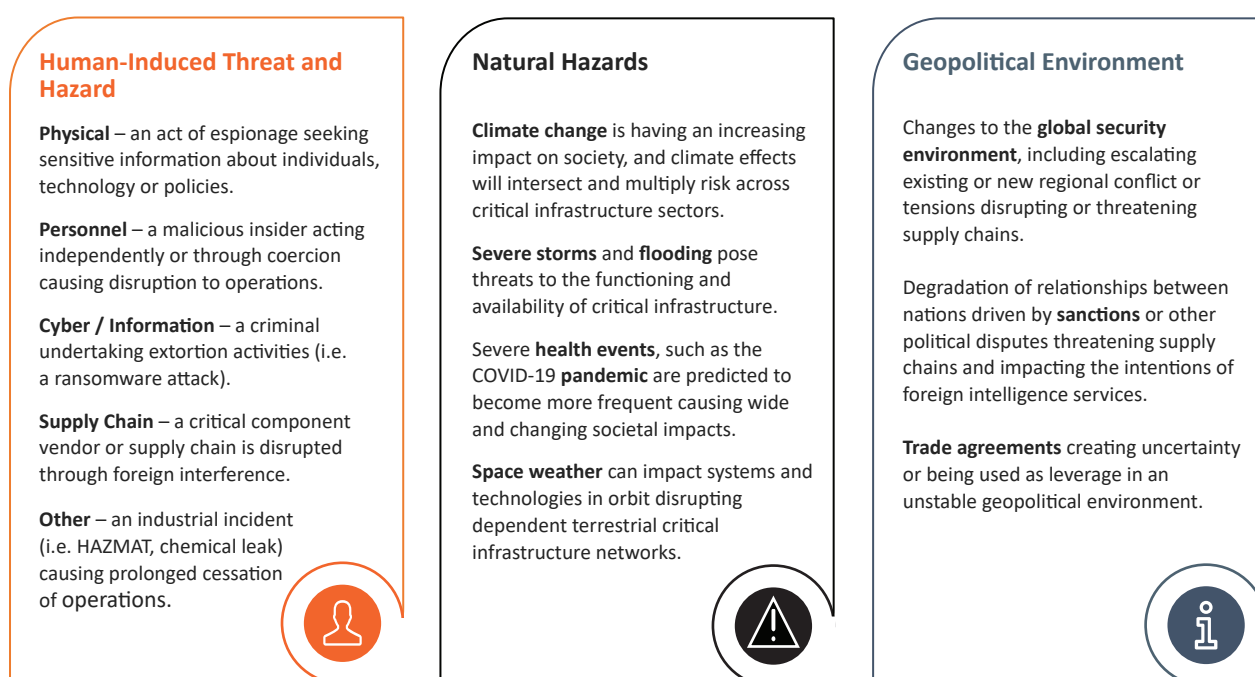


## Understanding threats and hazards for risk

### Identifying a threat and hazard landscape of the Financial Services and Markets 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 Financial Services and Markets Sector is an attractive target. 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 Financial Services and Markets Sector, driven by improvements in technology and the need to meet commercial outcomes, will become more interconnected. This means that stakeholders in the Financial Services and Markets Sector need to reevaluate risks regularly.



Natural hazards are becoming more frequent and intense; their impacts enduring and complex. The Financial Services and Markets Sector is susceptible to these kinds of hazards through damage to facilities, componentry, and broader impacts on the economy.

## Understanding sector-specific risks

This table outlines a select example of identified threat and hazard vectors that impact Financial Services and Markets 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 on financial networks, or to gain access to large quantities of sensitive personal and financial information.
	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 financial market networks and, current and future capabilities.
	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 financial services providers has the potential to halt the functioning of an asset for extended periods with the intent to extract financial benefits.
 NATURAL	Pandemic	<ul style="list-style-type: none"> <li>Confidentiality</li> <li>Availability</li> <li>Reliability</li> </ul>	Pandemics such as COVID-19 have the potential to greatly alter the functioning of society, with developments such as higher demand for online banking and payments.
	Severe weather event	<ul style="list-style-type: none"> <li>Availability</li> <li>Reliability</li> </ul>	With increasing extreme weather events, people in affected areas may experience difficulties in accessing cash and other payment systems, which could be compounded if weather impacts impede access to affected areas.
 PHYSICAL	Criminal activity	<ul style="list-style-type: none"> <li>Integrity</li> <li>Availability</li> <li>Reliability</li> </ul>	Criminal activity can cause damage through fraud, insider trading or stock market manipulation. These criminal activities can have broader consequences such as reputational damage and loss of income.
	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 cell towers, cell grids and wider networks to cause civil unrest.

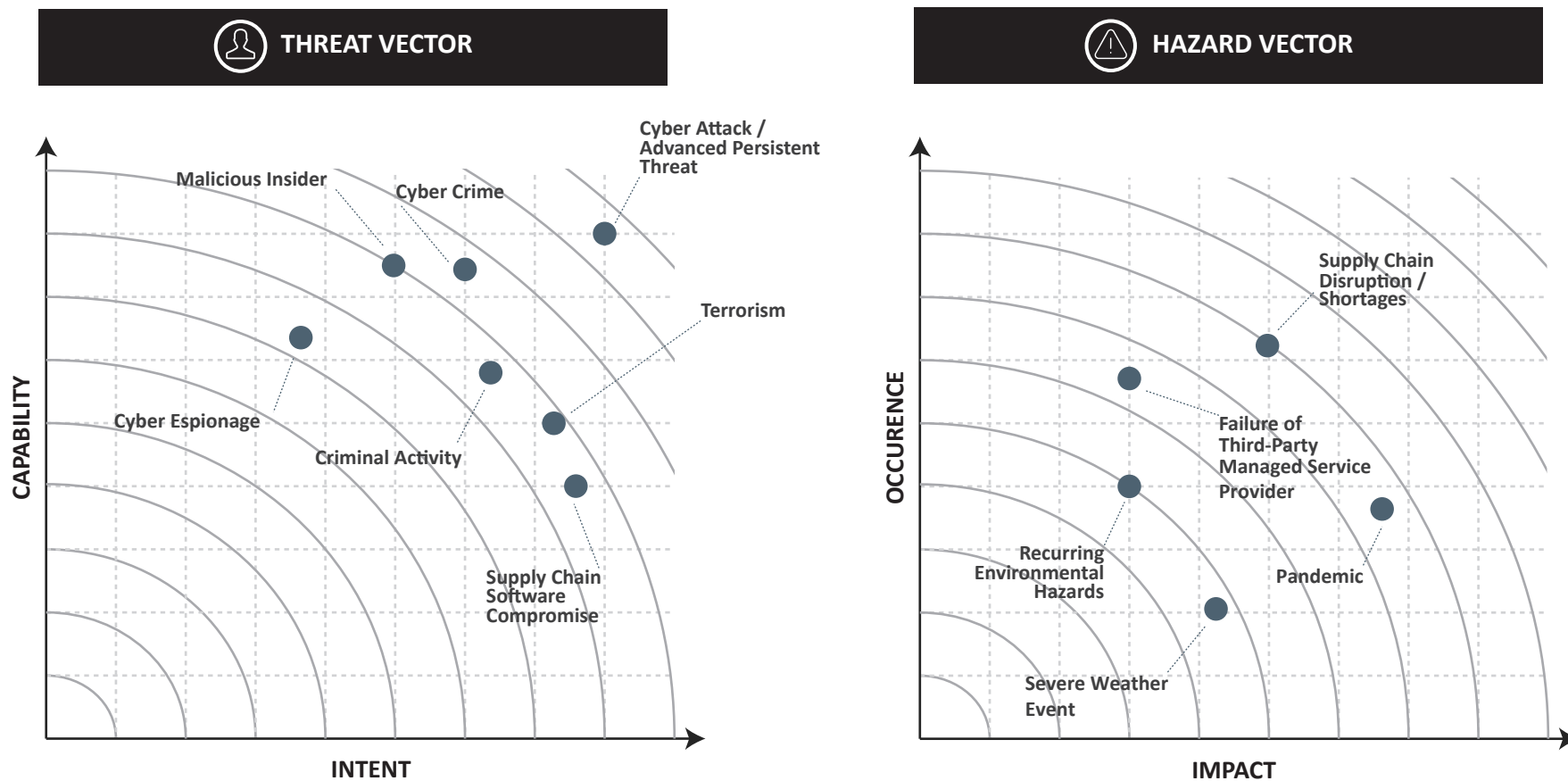


	Threat or Hazard Vector	Area of Potential Impact	Risk Scenario Considerations
 SUPPLY CHAIN	Failure of third-party managed service providers	<ul style="list-style-type: none"><li>• Availability</li><li>• Integrity</li><li>• Reliability</li></ul>	Third-party service providers relied upon to provide resources to the sector have the potential to fail, whether through management issues, capability shortcomings, or inadequate security practices.
	Compromise of software supply chain solutions	<ul style="list-style-type: none"><li>• Confidentiality</li><li>• Integrity</li><li>• Availability</li><li>• Reliability</li></ul>	Sectors that are largely service delivery and technology-based often rely on third-party components and solutions for business functions. These offloaded software processes often sit outside of the security standards of a given financial sector organisation, allowing threat actors to target lower security standards as a weak or vulnerable link into the organisation.
 PERSONNEL	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. For the Financial Services and Markets Sector, malicious insiders may also use inside knowledge to manipulate financial systems for financial gain.

## 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 Financial Services and Markets Sector asset, the disablement of its resources will cause issues downstream 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:

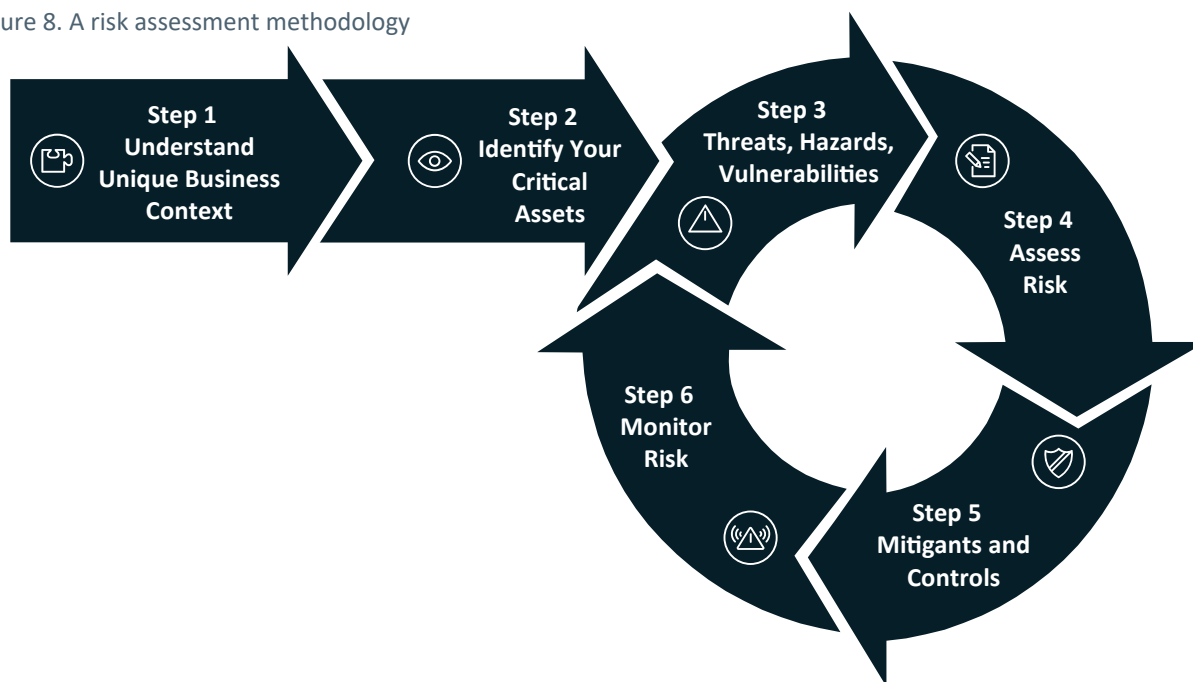
- Ease of implementation
- Cost-effectiveness
- Whether the action creates new risks and/or unintended consequences
- Environmental impacts (positive and negative)
- Multi-objective actions
- Long-term and short-term results
- Effectiveness
- Direct and indirect benefits
- Legal, regulatory, social and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



## Appendix – A risk assessment methodology

Financial Services and Markets 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 Financial Services and Markets 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.