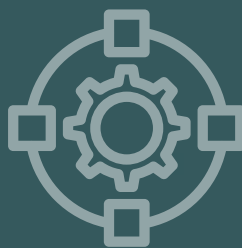




# South Australian Critical Infrastructure Resilience Strategy

2023-2026





<b>Version</b>	1.0
<b>Classification/DLM</b>	Public-I2-A2
<b>Authority</b>	State Emergency Management Committee pursuant to Section 9(1) (g) of the <i>Emergency Management Act 2004</i>
<b>Managed &amp; maintained by</b>	Department of the Premier and Cabinet
<b>Issued</b>	January 2024
<b>Minor amendments</b>	
<b>Disclaimer</b>	Users should ensure that they have the current version before taking action based on this strategy

# Contents

<b>Vision.....</b>	<b>2</b>
<b>Purpose .....</b>	<b>2</b>
OBJECTIVES.....	2
<b>Key Terminology .....</b>	<b>3</b>
<b>Effective identification and assessment .....</b>	<b>4</b>
Identifying CI .....	4
Understanding criticality and South Australia's framework for assessing infrastructure assets .....	5
Critical Infrastructure-High Risk (CI-HR) .....	6
Essential infrastructure (EI) .....	6
<i>Security of Critical Infrastructure Act 2018</i> .....	6
Actions .....	7
<b>Improved resilience planning and investment .....</b>	<b>8</b>
Encompassing an all-hazards approach to critical infrastructure resilience.....	8
Understanding risk appetite .....	9
Government resilience planning and frameworks in South Australia .....	9
Actions .....	9
<b>Enhanced collaboration and partnerships with owner-operators and government .....</b>	<b>10</b>
Partnerships and pathways to enhance relationships and coordinate arrangements .....	10
Facilitating cooperation and collaboration during an emergency .....	11
Actions .....	13

# Vision

South Australian Critical Infrastructure can withstand and recover from threats and disruptions.

# Purpose

To enhance the preparedness and resilience of the state's critical infrastructure (CI) systems in the face of all hazards and disruptions by developing a shared understanding of CI, prioritising risk assessment, investment in resilience measures, and collaboration.

## OBJECTIVES



**Effective identification and assessment:** by understanding the criticality of assets and supply chains through effective risk assessments, resilience efforts can be prioritised, and resources allocated effectively.



**Improved resilience planning and investment:** by identifying and implementing measures to enhance the robustness, redundancy, and flexibility of CI, resilience planning can be strengthened by encompassing an all-hazards approach and investment in CI systems.



**Enhanced collaboration and partnerships with owner-operators and government:** by fostering strong partnerships, information sharing and mapping interdependencies, South Australia can enhance its collective response and recovery capabilities after disasters.

# Key Terminology

Term	Acronym	Definition
All-Hazards	-	A hazard is a process, phenomenon or human activity that may cause loss of life, injury or other health impacts, property damage, social and economic disruption, or environmental degradation. South Australia's Emergency Management arrangements operate through an all-hazards approach, which assumes the functions and activities applicable to one hazard are often applicable to a range of hazards.
Critical Infrastructure	CI	Those physical facilities, systems, assets, supply chains, information technologies and communication networks which, if destroyed, degraded, compromised or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of South Australia as a State or affect South Australia's ability to support the conduct of national defence and ensure national security.
Critical Infrastructure High-Risk	CI-HR	State government-owned CI assets that if destroyed, disrupted, degraded, or rendered unavailable would significantly affect the reputation of the State or significantly reduce community confidence in the government's ability to effectively conduct business.
Essential Infrastructure	EI	Infrastructure that is not critical but would, if destroyed, degraded or rendered unavailable for an extended period, significantly impact the social or economic wellbeing of the people of South Australia.
Owner-Operator	-	Those who own or operate CI assets and are ultimately responsible for determining and managing risks to those assets.
Systems of National Significance	SoNS	A small subset of CI assets that are most crucial to the nation, by virtue of their interdependencies across sectors and potential for cascading consequences to other CI assets and sectors if disrupted.
Trusted Information Sharing Network	TISN	A network that provides a secure, non-competitive environment for CI owners and operators to share information and collaborate across the sector groups.



## Objective 1

# Effective identification and assessment

Disruption to critical infrastructure (CI) can have significant impacts on the economy. CI is defined as

*those physical facilities, systems, assets, supply chains, information technologies and communication networks which, if destroyed, degraded, compromised or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of South Australia as a State or affect South Australia's ability to support the conduct of national defence and ensure national security.*

When these infrastructures are disrupted impacts such as productivity losses, employment impacts and increased costs, lead to business interruptions impacting the economy which can erode investor confidence and financial markets. This can further dampen the economic growth and impede recovery efforts to the State.

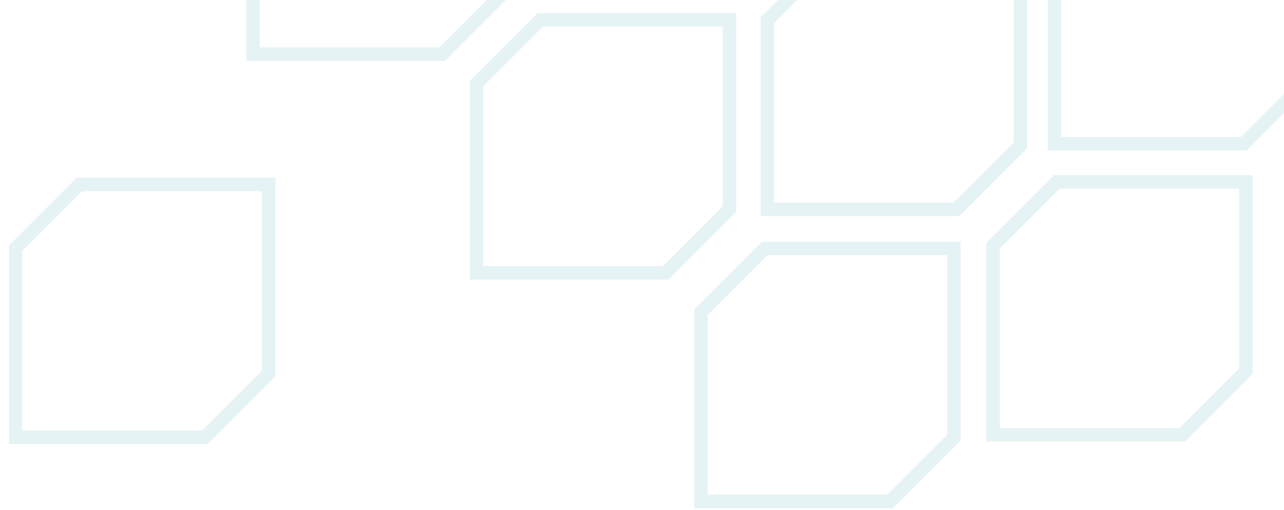
## Identifying CI

South Australia Police (SAPOL), Security Preparedness, is responsible for identifying and assessing CI for South Australia and for maintaining arrangements to work with owners and operators to assist in the provision of protective security guidance to owners-operators of CI.

Once assessed, owner-operators of CI have ultimate responsibility and are best placed to determine and discharge their own legal obligations and manage the risks to the operation of CI assets, according to the level of risk and criticality associated with that asset. The government's role in supporting entities to perform these functions includes identifying CI assets and assessing risk appetite.

The government has an expectation that owner-operators:

- maintain an awareness of their operating environment and potential threats
- provide adequate security for their assets, based on threat and identified risk
- actively apply risk management and mitigation techniques to their planning processes
- conduct regular reviews of risk and develop business continuity plans, including identifying interdependencies
- assessments and security, emergency and contingency plans
- periodically test plans (at least every five years) to determine if adequate
- conduct training and exercise their security, emergency and contingency plans
- participate in government exercises to assist in harmonising prevention and preparedness, response and recovery arrangements with relevant controlling agencies.



## Understanding criticality and South Australia's framework for assessing infrastructure assets

Many assets will be critical to an entity's operations, however not all will meet a threshold for State or national interest. South Australia's criticality framework and methodology for assessing critical assets considers several factors to assess an asset's criticality and is directly proportionate to the consequence to the State and the well-being of its people. The severity of consequence of an asset's failure is determined by reviewing the impact to the community and the State's business activity, as well as the duration of the failure.

Considerations of the security, economic impact, and political impact of assets are included in the methodology as separate considerations in conjunction with risk and criticality. The level of criticality determines how often the asset's risk assessment is reviewed.

The below table describes the levels of CI across South Australia.

### State infrastructure criticality ratings

Vital	Loss or compromise could result in abandonment or long-term cessation of the asset and will require assistance nationally. Alternative services and/or facilities cannot be provided by the State.
Major	Services and/or facilities are severely disrupted, major restrictions will apply to the State and the service/facility will likely require assistance nationally.
Significant	Services and/or facilities would be available after a severe disruption but with restrictions. The service may be provided within this State, but reliance may be placed nationally.
Low	If disrupted services and/or facilities can be provided within the State with limited loss of function.
Insignificant	Services and/or facilities can be provided within the State with no loss of function.

## **Critical Infrastructure-High Risk (CI-HR)**

Critical Infrastructure of High Risk (CI-HR) is a specific designation of government-owned CI assets in South Australia that determines the requirement of increased physical security measures, including the need for deployment of Police Security Officers (PSO)

The process for the designation of CI-HR assets is incorporated into the South Australian Protective Security Framework (SAPSF) under PHYSEC1: Physical Security.

## **Essential infrastructure (EI)**

The protections and requirements applied to CI do not apply to Essential Infrastructure (EI). In most cases, disruption of or interference with an EI asset would result in an isolated local and/or sector impact, rather than impact on the State as a whole. Under South Australia's current framework, EI is understood as low or insignificant criticality.

## ***Security of Critical Infrastructure Act 2018***

At the national level, CI assets are privately declared by the Minister for Home Affairs under the *Security of Critical Infrastructure Act 2018* (SoCI Act). Protection arrangements and requirements for assets declared under the SoCI Act are administered and enforced by the Australian Government. A small subset within this cohort are declared Systems of National Significance (SoNS) due to their interdependencies across sectors and potential for cascading consequences if disrupted.

For more information on the SoCI Act, nationally declared CI and SoNS visit [www.cisc.gov.au](http://www.cisc.gov.au)



## Actions

- 1** Conduct a thorough review and establish processes so entities can more proactively undertake risk assessments, thereby streamlining CI designation requests and improving decision making. The purpose of this process is to ensure that entities have the appropriate level of support, and that the SA Government is aware of ways in which to improve resilience relevant to assets.
- 2** Improve the methodology of formal CI assessments in South Australia to reflect an all-hazards approach by expanding on the types of assets included.
- 3** Explore the feasibility of introducing legislation to assist the government to prepare and respond to incidents which may affect CI. Any potential legislation developed concerning CI in South Australia should not contradict or duplicate the rules under the SoCI Act and should not place unnecessary additional burden on operators of CI.
- 4** Establish a defined threshold for EI, with its own scale of criticality.



## Objective 2

# Improved resilience planning and investment

South Australia's risk profile is continuously changing and increasingly challenging to navigate. Changes such as on evolving technology, population growth, climate change and increasing interconnectedness of systems alter operational threats and challenges to CI across all sectors.

In addition to natural hazards, South Australia is becoming a more prominent player in global affairs, increasing the likelihood of being targeted by foreign actors. South Australia is more connected to the world than ever before, due in part to increased digitalisation of our infrastructure and government systems. By improving our CI resilience, South Australia can offer security and stability to industries, allowing us to strengthen our economy and further become a partner of choice in an insecure world. This means South Australia must have a strong digital regulatory environment, and its own set of robust defences to protect CI.

## Encompassing an all-hazards approach to critical infrastructure resilience

Critical infrastructure resilience (CIR) refers to the capacity of CI to withstand disruption, operate effectively in crisis, and deal with and adapt to unexpected shocks and anticipated and long-term stresses. The aim of CIR is the continued operation of CI in the face of all-hazards, including extreme acts and natural disasters. When not mitigated appropriately, long-term stresses exacerbate the impacts of shock events. CIR does not only refer to physical infrastructure assets, networks and systems but also encompasses organisations, processes, and the South Australian community's ability to withstand emergencies and adapt to a new normal after a major disruption. For those emergencies that cannot be prevented, CIR will improve the response and recovery of such events, resulting in minimisation of the consequences to the social, economic and built environments.

### Shocks



Natural disasters



Extreme weather



Disease outbreaks



Terrorism



Cyber attacks

### Stresses



Climate change



Ageing infrastructure



Mental health



Drought



Poverty

## Understanding risk appetite

The threats and hazards to South Australia must be understood to understand the risk profile of a particular CI asset. Owner-operators of CI must understand the risk appetite of their asset and the level of priority associated with the level of risk as they are ultimately responsible for determining and managing risks to their operations. This is achieved through appropriate risk management practices including the development and review of business continuity plans, and the provision of adequate security for their assets.

## Government resilience planning and frameworks in South Australia

SAPOL maintains a secure database of profiles prepared with owners and operators of SA CI assets that are recommended to be reviewed and updated regularly. These profiles include a list of relevant available plans maintained and held by the owners and operators. The SA Government has a number of policies and frameworks that aim to address various risks across the sectors. These include the State's future infrastructure needs, adapting to a changing climate and creating a shared understanding of disaster resilience.

### Actions

- 1** Develop guidance to understand and address climate risks on CI to assist responsible entities to understand the physical and transition climate risks when planning, designing, constructing, and operating CI.
- 2** Incorporate CI resilience testing into regular training and exercises to prepare agencies for emergencies and disruptions. Exercises will help to identify gaps in planning, improve coordination and enhance decision making under stress.
- 3** Investigate what further security measures (protective or cyber focussed) are required for CI-HR and vital CI assets to mitigate vulnerabilities.
- 4** Improve the transparency of the ownership and operational control of CI. The influence of parent companies on the ownership and operational control of CI assets needs to be understood in order to better manage risks, including that of foreign interference.



## Objective 3

# Enhanced collaboration and partnerships with owner-operators and government

Leveraging the collective strengths and resources of owner operators and government, CI can become more resilient, adaptive and sustainable, fostering economic stability and long-term prosperity. Owner-operators possess specialised knowledge and expertise in operating and maintaining CI systems, making them valuable partners in identifying vulnerabilities and implementing effective risk management strategies. By working closely with government, owner-operators can contribute their insights to the development of robust resilience plans and the implementation of proactive measures. This collaboration can assist with identifying and addressing potential risks before they become crises, ensuring the continuity of services and minimising disruptions to the economy. These partnerships can also facilitate the efficient allocation of resources, enabling timely implementation of infrastructure projects that stimulate economic growth.

### Partnerships and pathways to enhance relationships and coordinate arrangements

CI assets often span across state, territory and international borders and as a result it is vital that industry and governments work together to ensure that resilience-building efforts are targeted, coordinated and complement one another. This includes enhancing cross-sector arrangements and improving transparency, collaboration and representation of owner-operators and government.

### Trusted Information Sharing Network (TISN)

Several key entities work together to represent South Australia in the Trusted Information Sharing Network (TISN), the Australian Government's primary engagement mechanism with industry on CI. The TISN holds regular meetings for the CI sector groups for sharing information and resilience building initiatives relevant to their sector.

For more information about the TISN and how to join visit [www.cisc.gov.au](http://www.cisc.gov.au).





## **Facilitating cooperation and collaboration during an emergency**

### **National Coordination Mechanism (NCM)**

The National Coordination Mechanism (NCM) is a permanent response tool in the Australian Government Crisis Management Framework (AGCMF) which clarifies how CI owner-operators interact with emergency management arrangements. The NCM was designed to be a flexible tool to ensure coordination, communication and collaboration occur between the Australian, state and territory governments and, if required, the private sector during a crisis. The NCM may be activated to coordinate a response to assist or assess impacts to CI assets that span across borders.

South Australia may request that the NCM is activated in response to a disruption to South Australian CI if national capabilities or assistance is required. Activation and engagement with the NCM for an emergency based in South Australia is the responsibility of the control agency in conjunction with the Department of the Premier and Cabinet.

## **Mapping interdependencies**

Today's modern, digital and highly technical society involves complex networks, communications and infrastructure, which are all linked and interdependent to some extent. During normal operation, interdependencies support efficiency and operational capacity.

During an emergency event, interdependencies determine how a disruption to one CI asset may affect others, depending on the asset, impact, and duration.

Vulnerabilities in these interdependencies targeted by malicious actors could result in significant consequences for the sector, State, and the nation.

Interdependency mapping reveals the interconnectedness of South Australia's supply chains, networks and systems and exposes vulnerabilities.


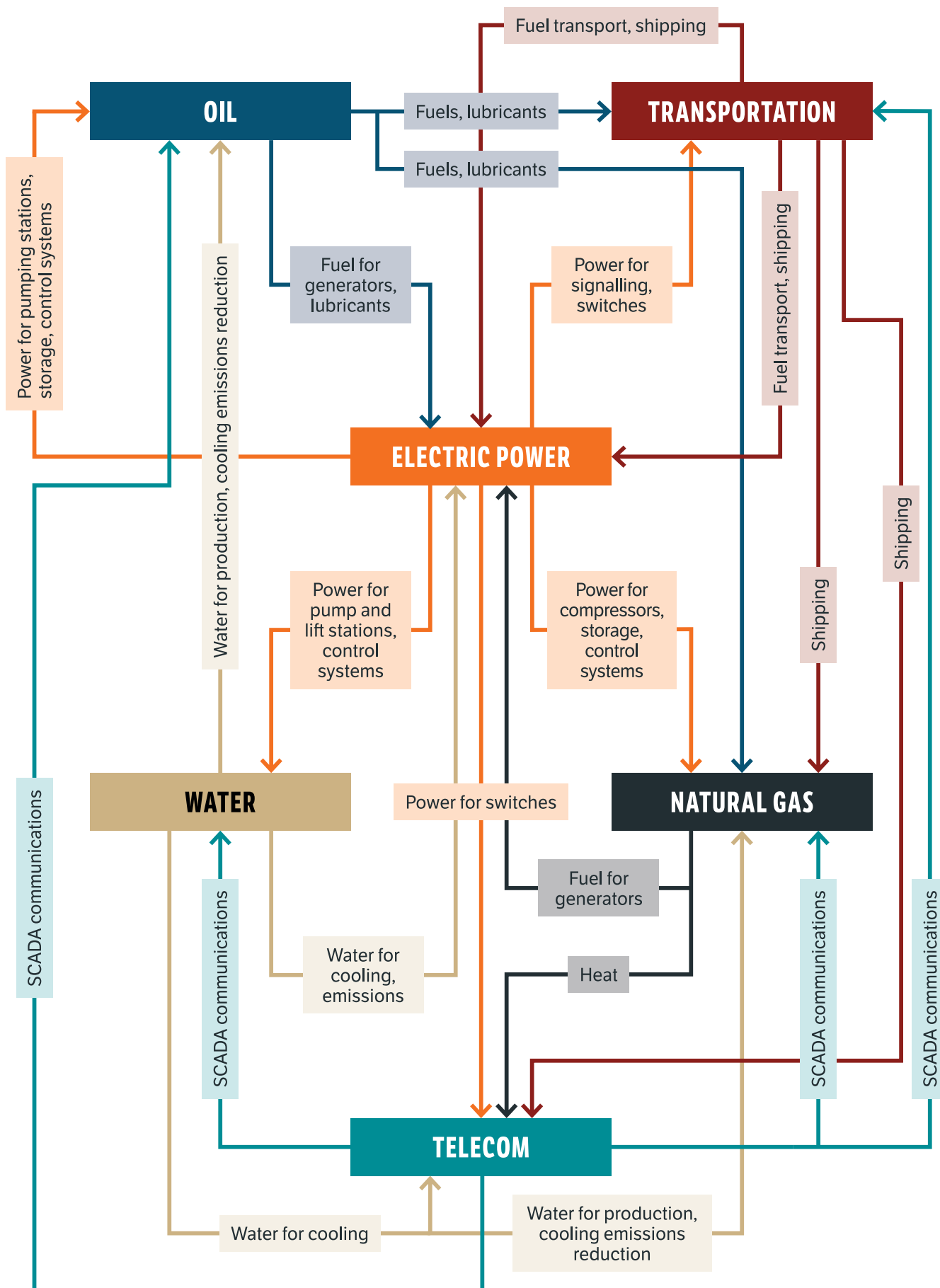


Figure 1: CI Interdependencies



## Actions

- 1** Establish a cross-sector CI working group as a mechanism for SA Government agencies that own state and national CI assets to share information, knowledge and experience in meeting the obligations of the SoCI Act.
- 2** Improve interdependency mapping between agencies, to reveal the interconnectedness of South Australia's supply chains, networks and systems and expose vulnerabilities. The identification and analysis of vulnerabilities and system-wide risks will increase the potential for more effective sharing of risk, contributing to overall resilience across the state.
- 3** Review how the CI list is used and maintained in South Australia.
- 4** Establish and review business continuity plans and back up infrastructure to ensure operational continuity during disruptions which may include back up power sources, data backup, alternative supply chains and communication networks.



**[www.security.sa.gov.au](http://www.security.sa.gov.au)**



With the exception of the Piping Shrike emblem, other material or devices protected by Aboriginal rights or a trademark, and subject to review by the Government of South Australia at all times, the content of this document is licensed under the Creative Commons Attribution 4.0 Licence. All other rights are reserved.

© Crown in right of the State of South Australia.

2024 | FIS 1004643

