SA Power Networks | ENERVEN™

Cyber Security Strategy 2025 2030

Contents

Acknowledgement of Country

In the spirit of reconciliation, SA Power Networks Group and Enerven acknowledges the multiple Traditional Owners of the lands that host the South Australian electricity network and their connections to land, sea and community. We would also like to pay our respects to Elders past and present and acknowledge that these are living cultures.

The visual centrepiece of our first Reconciliation Action Plan is Empowering South Australia, by Presten Warren, an artist and proud Wirangu/Dieri/Kokatha/Mirning man.

Cover: Adelaide city skyline illuminated at night, looking toward the Adelaide Hills.

Foreword

Welcome to the SA Power Networks Group Cyber Security Strategy 2025–2030

As South Australia's sole distributor of electricity, we are an essential infrastructure organisation. SA Power Networks Group has two key businesses: SA Power Networks, which manages the regulated electricity distribution network serving South Australia, and Enerven, a specialist service provider in the competitive energy and telecommunications sectors.

Like our colleagues around Australia and the world, we are operating within an increasingly complex and evolving digital and cyber threat landscape. The risks to cyber security are multifaceted and evolving and, should they materialise, could cause significant harm to our operations, and the customers and communities we serve.

A robust, comprehensive and responsive cyber security strategy and practice is essential to the safe and secure operation of both businesses, and to our overall mission of empowering South Australia.

This strategy represents the culmination of several years' work to understand, forecast, prepare for and manage safe and secure electricity supply for South Australia for the next five years, and beyond. It contributes to the achievement of SA Power Networks Digital and Data Strategy and will guide our work in this crucial space.

Matthew Pritchard
Chief Digital Officer, SA Power Networks Group

To learn more about how SA Power Networks is leading in the cyber security space, read our latest Cyber Security Annual Report.

For the purposes of this strategy, reference to SA Power Networks is inclusive of Enerven.

SA Power Networks

Snapshot

9679GWh

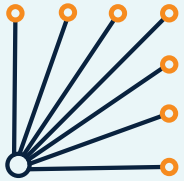
of electricity supplied every year

1.7 million

customers

930,000

homes and businesses empowered

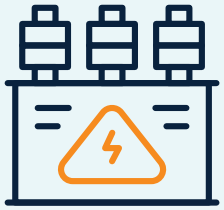


178,000km²+

covered by our network

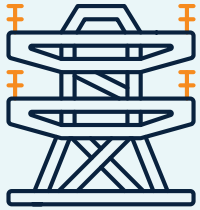
2800

employees in 40+ sites



77,000

transformers



406

zone substations

Award-winning

cyber security team

2025 2030 Strategy overview

The Cyber Security Strategy 2025–2030 comprises 12 key initiatives for controlling the risks in our environment

Monitoring and managing these threats and critiquing and optimising the robustness of our initiatives is an ongoing focus for SA Power Networks as we do the vital work of empowering South Australia.

The strategy considers and extends on the Australian Energy Sector Cyber Security Framework (AESCSF) with a threat and risk-based approach to effectively address SA Power Networks needs.

This strategy will enable us to identify any gaps in our security measures and plan or actively strengthen our overall cyber resilience by prioritising our efforts and allocating resources where they are needed most. It ensures that our cyber security measures effectively mitigate our key identified cyber security risks and align with our organisational risk tolerance.

At the same time as implementing the Cyber Security Strategy 2025–2030, we will conduct regular and ongoing cyber security operations to ensure the maintenance and uplift of SA Power Networks network security.

These include →

- **Core and substation firewalls** will help to provide secure and reliable connectivity and ensure that only legitimate communications are possible across our IT network.
- **A centralised firewall management system** will enable consistent policy application across all firewalls, and act as a ‘single fix’ to decisively limit any security threats across SA Power Networks.
- **Security monitoring and threat detection systems** will enhance our ability to detect and identify cyber threats using AI and other technologies, enabling 24/7 detection and response.
- **Authentication and certificate systems** will make trust integral to our communications, giving users confidence in the legitimacy of our identity and requirements, and vice versa.
- **A vulnerability management platform** will reduce security vulnerabilities by uplifting our threat intelligence and our visibility into activities, including anomalous behaviour, within our cyber environment.
- **A multi-factor platform and tokens** will achieve greater integrity in systems access and authentication and lower our overall risk of compromise.
- **Demilitarised jump hosts and privileged access workstations** will enable separation of duties, ensuring staff with heightened levels of access to sensitive resources are subject to higher levels of scrutiny and preventative controls, reducing our risk of compromise.

We are also committed to remaining vigilant to new threats, and to exploring new opportunities in the fast-paced, complex and ever-evolving digital environment we operate within.

Risk overview

This strategy addresses SA Power Networks 10 key cyber risks

1. Environmental compromise

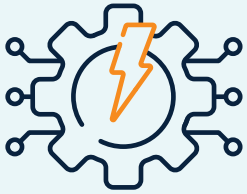
Failure of cyber controls to prevent catastrophic or damaging compromise of SA Power Networks systems, data and digital assets.

3. Loss of sensitive data

Failure to prevent sensitive data being exfiltrated (extracted) or erased by an unauthorised party.

2. Loss, abuse or misuse of credentials

Unauthorised use of a digital identity to gain access to systems or data assets by internal or external actor.



4. Critical systems failure

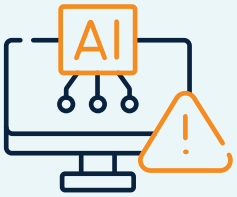
Catastrophic or damaging failure of critical systems, jeopardising SA Power Networks ability to function reliably and safely.

5. Supply chain failure

Compromise of third-party suppliers leading to unacceptable cyber security risks and the introduction of new cyber threats.

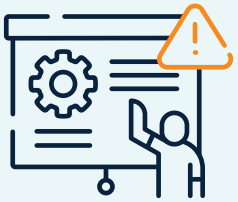
8. Vulnerabilities in technology

Failure to detect, identify or remediate security or operational vulnerabilities that open the door to exploitation or compromise.



6. Inadequate response to emerging technologies

Failure to manage risks relating to the arrival and adoption of new and emerging technologies.



9. Poor cyber culture

Compromise due to a lack of required cyber security knowledge, education, support, oversight or awareness.

7. Failure of cyber governance

Breach, interruption or other compromise due to inadequate policies, processes and practices for digital asset and systems management.

10. Public exposure

Deliberate sharing of SA Power Networks information or data in the public realm that could potentially be used against us.

Key initiatives

Twelve key initiatives underpin our risk-based approach to cyber security

Each key initiative addresses one or more of the key risks to SA Power Networks cyber security and involves multiple, complex and intersecting controls and actions. The initiatives will be deployed in an ongoing way or at various strategic points in the five-year period, and will be subject to ongoing monitoring, review and adjustment or redirection.

1. Uplift tool of trade devices

(2025, 2027–2028)

To ensure a secure environment for performing sensitive tasks.

2. Increase third-party security monitoring

(2025–2026)

To minimise risk exposure and maintain a higher level of trust and confidence in third-party relationships.

3. Build resiliency into everyday operations

(2025–2030)

To ensure SA Power Networks can withstand and rapidly recover from disruptions and outages.

4. Continuously optimise cyber security operations

(2025–2030)

To improve the prevention, detection, assessment, and remediation of cyber incidents.

5. Cultivate a proactive cyber security culture

(2025–2030)

To strengthen SA Power Networks resilience.

6. Embed security in operational technology

(2026–2029)

To identify, mitigate and manage OT-specific cyber risks and protect critical assets.

7. Introduce security measures for non-SA Power Networks devices

(2026–2030)

To ensure all end user devices meet a secure baseline.

8. Strengthen information protection

(2026–2030)

To optimise how we safeguard valuable data assets.

9. Enhance identity and access controls

(2027–2029)

To build defensible SA Power Networks systems and infrastructure.

10. Manage risk across the software development lifecycle

(2028–2029)

To mitigate security risks and incidents end to end.

11. Centralise identity management

(2029–2030)

To build user-led cyber security hygiene and reduce risk.

12. Introduce network detection and response capabilities

(2029–2030)

To increase visibility of abnormal network activity and threats.

1. Uplift tool of trade devices

To ensure a secure environment for performing sensitive tasks

Tool of trade (ToT) devices are used for specialised OT infrastructure access and maintenance. Customised to support legacy and non-standard interfaces and software that sometimes require the use of end-of-life operating systems, a comprehensive ToT device assessment to highlight any control deficiencies will help us to identify, evaluate and respond to any security gaps.

Actions

1. Identify any control deficiencies and develop a standard set of controls for ToT devices.
2. Implement appropriate security measures to address any identified risks.
3. Use controls to establish a baseline for future deployment and ongoing monitoring of ToT devices.
4. Develop framework for tracking and evaluating the effectiveness of implemented controls, identifying any emerging security risks, and promptly addressing them to maintain a robust and secure operational environment.
5. Establish a metrics framework for this initiative that includes qualitative and quantitative metrics, to evaluate its effectiveness and support progress reporting.

Risks managed

Environmental compromise

Loss of sensitive data

Vulnerabilities in technology

When

2025, 2027–2028

2. Increase third-party security monitoring

To minimise risk exposure and maintain a higher level of trust and confidence in third-party relationships

Managing and minimising the increasingly complex risks associated with third-party supply chains, such as the adoption of cloud technology and service as a solution (SaaS), software purchases and third-party providers and suppliers, demands robust and continuous monitoring. This will include comprehensive and ongoing real-time assessment of third-party security, a deeper understanding of any risk exposure, and regular review.

Actions

1. Develop a comprehensive risk score for our vendors based on publicly available information.
2. Leverage third-party monitoring services to access real-time insights and notifications regarding any breaches or security incidents involving the third-party organisations.
3. Regularly review and reconsider third-party relationships.
4. Establish a metrics framework for this initiative that includes qualitative and quantitative metrics, to evaluate its effectiveness and support progress reporting.

Risks managed

Loss of sensitive data

Critical systems failure

Supply chain failure

When

2025–2026

3. Build resiliency into everyday operations

To ensure SA Power Networks can withstand and rapidly recover from disruptions and outages

IT resiliency is the ability of IT systems and infrastructure to withstand, adapt to, and recover from disruptions or outages. Optimising SA Power Networks IT resiliency will be an ongoing process involving proactive planning, preparation and testing to ensure we maintain business continuity and customer service in the face of unexpected events.

Risks managed

Loss of sensitive data

Critical systems failure

Actions

1. Review systems and reassess for critical or non-critical status.
2. In alignment with the National Institute of Standards and Technology (NIST)'s Security and Privacy Controls for Information Systems and Organisations, develop robust contingency plans, determine the effectiveness of current resilience controls and identify potential weaknesses. This action will include checklists, walk-through and tabletop exercises, simulations (parallel or full interrupt), and comprehensive exercises.
3. Develop a comprehensive testing framework. This action will specify:
    a. testing lifecycle for all business-critical applications and systems
    b. an uplift of supporting artefacts that outlines interconnectivity and interdependency
    c. regular evaluation of critical applications and systems
    d. regular reassessment of their significance in SA Power Networks broader business continuity framework.
4. Establish a metrics framework for this initiative that includes qualitative and quantitative metrics, to evaluate its effectiveness and support progress reporting.

When

2025–2030

4. Continuously optimise cyber security operations

To improve the prevention, detection, assessment and remediation of cyber incidents

Formally integrating SA Power Networks IT security and IT operations functionality will enhance our overall security posture while ensuring efficient and reliable system performance. This approach is known as SECOPS (SECurity OPerationS), and involves applying real-time practices, tools and processes for best-practice monitoring, detecting, and responding to security threats alongside systems maintenance.

Risks managed

Environmental compromise

Loss, abuse or misuse of credentials

Loss of sensitive data

Inadequate response to emerging technologies

Vulnerabilities in technology

Public exposure

Actions

1. Implement a cloud security platform to enable the identification of vulnerabilities and misconfigurations specific to the cloud environment, such as unprotected storage, and to minimise the chances of attackers exploiting these cloud-related risks. This action will include:
    a. Appropriate gap analysis work
    b. Holistic vulnerability intelligence, centralisation, integration, automation and training to uplift knowledge within the team.
2. Improve how we collect, store, utilise and share threat intelligence.
3. Integrate a comprehensive threat-intelligence platform to enhance our proactive threat detection capabilities and strengthen our incident response strategy. This action will include:
    - Acquiring specific threat feeds tailored to critical infrastructure and the energy sector
    - Embedding an additional FTE in the SECOPS team to assist in processing and automating threat intelligence.
4. Establish and maintain clear and well-defined states of operation for both the IT and OT environments. This action will include:
    a. Developing a detailed understanding of our assets and their priorities
    b. Documenting the architecture and topologies of each state
    c. Developing criteria for triggering a state change, specifying authorities for approval, checklists for moving between states, and how long we can operate in each state and monitoring required during each state.
5. Identify and close any endpoint detection gaps in our system.
6. Establish a metrics framework for this initiative that includes qualitative and quantitative metrics, to evaluate its effectiveness and support progress reporting.

When

2025–2030

5. Cultivate a proactive cyber security culture

To strengthen SA Power Networks resilience

Cyber security is not just a technical challenge; it is a human one. By implementing a comprehensive and inclusive security awareness program that involves all our people and teams, we will be able to identify our top human behaviour risks, introduce key behaviours or strategies to manage those risks, enable and change those key behaviours both individually, and organisation wide, and cultivate a robust and protective cyber security culture across SA Power Networks.

Risks managed

Loss, abuse or misuse of credentials

Inadequate response to emerging technologies

Poor cyber culture

Public exposure

Actions

1. Draw on the SANS Security Awareness Maturity Model roadmap to deliver this initiative.
2. Actively collaborate with other departments, partners and collaborators from various areas to leverage their expertise and resources in enhancing cyber awareness.
3. Deliver ongoing reinforcement training, including lunch-and-learn sessions, regular internal news articles, and education on the latest threats and scams.
4. Identify business areas that pose an increased or unique human risk and implement targeted awareness initiatives to address and uplift these areas.
5. Establish a formal incentive program to recognise individuals, groups or departments that excel in cyber security or demonstrate key behaviours aligned with industry best practices.
6. Empower staff across the business to become cyber security awareness ambassadors, fostering a culture of proactive security awareness and incident reporting.
7. Establish a metrics framework for this initiative that includes qualitative and quantitative metrics, to evaluate its effectiveness and support progress reporting.

When

2025–2030

6. Embed security in operational technology

When

2026–2029

To identify, mitigate and manage OT-specific cyber risks and protect critical assets

Security has historically been managed differently within IT systems and OT environments. Embedding a specialised cyber security team within the SA Power Networks OT environment will help to align and strengthen OT with IT and enhance our overall security. The Cyber Security team will be closely aligned with the OT support teams and play a crucial role in identifying, mitigating and managing cyber risks specific to OT. When an incident crosses from IT to OT or vice versa, collaboration between these two teams will be paramount, as will the ability to support each other in the event of any incident.

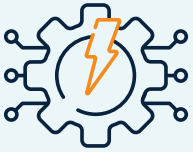
Actions

1. Embed a dedicated cyber security team within the SA Power Networks OT environment.
2. Map and review cyber security risk visibility, incident response and OT cyber security knowledge within the OT environment.
3. Develop shared governance models and strategies that consider the requirements of IT systems and the OT environment.
4. Establish protocols for managing risks, threats and incidents, including exploring opportunities for shared management.
5. Establish a metrics framework for this initiative that includes qualitative and quantitative metrics, to evaluate its effectiveness and support progress reporting.

Risks managed

Environmental compromise

Loss of sensitive data



Critical systems failure

Failure of cyber governance

Inadequate response to emerging technologies

Poor cyber culture

7. Introduce security measures for non SA Power Networks devices

To ensure all end-user devices meet a secure baseline

The widespread adoption of bring your own device (BYOD) working presents a significant cyber risk, as BYOD devices serve as an uncontrolled entry point for accessing SA Power Networks data and systems. Taking a proactive approach to BYOD security will help to safeguard our data, systems and infrastructure while allowing employees to leverage the benefits of BYOD in their work environment.

Risks managed

Environmental compromise

Loss, abuse or misuse of credentials

Loss of sensitive data

Actions

1. Develop an ongoing framework for identifying any areas of weakness introduced by BYOD use and implementing appropriate controls to effectively close any gaps.
2. Support BYOD users to install purpose-built endpoint detection and control software on their devices, ensuring better visibility and control over potential threats.
3. Enable flexible work practices while maintaining a robust security posture.
4. Establish a metrics framework for this initiative that includes qualitative and quantitative metrics, to evaluate its effectiveness and to support progress reporting.

When

2026–2030

8. Strengthen information protection

To optimise how we safeguard valuable data assets

Strengthening how we protect information assets with a robust framework for protecting them will enable us to uphold the confidentiality, integrity and availability of sensitive data. The framework will combine automated asset identification, targeted security controls and a data loss prevention (DLP) solution and involve high-level oversight, automation and coordination of information assets and business assets that contain or utilise information.

When

2026–2030

Actions

1. Automate identification of information assets and business assets that contain or utilise information to gain a comprehensive view of our assets and their associated security requirements.
2. Implement asset-specific security controls best suited to their unique characteristics and risk profiles to ensure effective protection of our information assets.
3. Implement a comprehensive DLP solution to achieve granular control over movement and handling of sensitive information.
4. Establish a robust framework for ongoing protection of SA Power Networks information assets.
5. Establish a metrics framework for this initiative that includes qualitative and quantitative metrics, to evaluate its effectiveness and support progress reporting.

Risks managed

Environmental compromise

Loss of sensitive data

Inadequate response to emerging technologies

Public exposure

9. Enhance identity and access controls

To build defensible SA Power Networks systems and infrastructure

Enhancing our identity and access controls by implementing a zero trust architecture (ZTA) security model will prompt our system to assume all internal and external resources are potentially compromised, and to require high-level identity authentication and authorisation before it grants access. ZTA's stringent identity controls, along with principles of least privilege and minimum necessary access, will help to safeguard SA Power Networks systems, infrastructure and customers.

Actions

1. Implement a ZTA security model to manage insufficient separation between critical and non-critical systems within the same zone.
2. Micro-segment the network into isolated segments to ensure that critical systems reside in dedicated spaces, distinct from non-critical counterparts.
3. Increase our ZTA maturity to the advanced and optimal levels of the CISA Zero Trust Maturity Model. This action will focus on five key functions: identity, devices, network, applications and workloads, and data.
4. Apply the principles of least privilege and minimum necessary access.
5. Implement a continuous monitoring and response capability, where any anomalous behaviour is quickly detected and acted upon.
6. Establish a metrics framework for this initiative that includes qualitative and quantitative metrics, to evaluate its effectiveness and support progress reporting.

Risks managed

Environmental compromise

Loss of sensitive data

Supply chain failure

Inadequate response to emerging technologies

Vulnerabilities in technology

When

2027–2029

10. Manage risk across the software development lifecycle

To mitigate security risks and incidents end to end

Taking a structured and highly risk-averse approach to software building and development will enable us to identify and address security vulnerabilities early on, reducing risks and helping to ensure the final product is secure. To achieve this, we will apply the principles and practices of the Secure Software Development Lifecycle (SSDLC) approach across the spectrum of software development: governance, design, implementation, verification and operations.

Actions

1. Create a sustainable program through standards and guidelines that incorporates SSDLC practices by drawing on Open Web Application Security Project (OWASP)'s Software Assurance Maturity Model (SAMM) V2.
2. Implement security testing tools and processes, as well as verification testing.
3. Upskill personnel with regular training and education so they are able to identify and mitigate security risks throughout the software development lifecycle.
4. Establish a metrics framework for this initiative that includes qualitative and quantitative metrics, to evaluate its effectiveness and support progress reporting.

When

2028–2029

Risks managed

Environmental compromise

Loss of sensitive data

Critical systems failure

Inadequate response to emerging technologies

Vulnerabilities in technology

Poor cyber culture

11. Centralise identity management controls

To build user-led cyber security hygiene and reduce risk

Centralising our identity management practices and procedures with a robust, streamlined and centralised identity management system will improve SA Power Networks cyber security hygiene and reduce cyber risk. We will introduce a digital identity solution (ie MyID) to support our people and teams to manage their personal and professional identity securely, including how they access our services or systems. It will bring all user-driven actions together in a single user interface, reducing touch points and flowing into our identity automation suite to be delivered to connected endpoints.

Actions

1. Explore MyID solution options to identify the best fit solution for SA Power Networks.
2. Implement preferred MyID solution.
3. Establish a metrics framework for this initiative that includes qualitative and quantitative metrics, to evaluate its effectiveness, and to support progress reporting.

Risks managed

Loss, abuse or misuse of credentials

When

2029–2030

12. Introduce network detection and response capabilities

To increase visibility of abnormal network activity and threats

Network detection and response (NDR) solutions provide advanced capabilities for analysing network communications, detecting threats, investigating anomalous behaviours, and identifying risky activities that are typical of attack behaviour. As part of uplifting our cyber security controls, we will investigate and implement an NDR solution to enhance our network visibility and monitoring capabilities, allowing us to proactively detect and respond to potential threats and anomalous activities within our network infrastructure, and better protect our critical assets and sensitive information from sophisticated cyber threats.

Actions

1. Explore NDR solution options to identify the best fit solution for SA Power Networks.
2. Implement preferred NDR solution.
3. Establish a metrics framework for this initiative that includes qualitative and quantitative metrics, to evaluate its effectiveness and to support progress reporting.

Risks managed

Environmental compromise

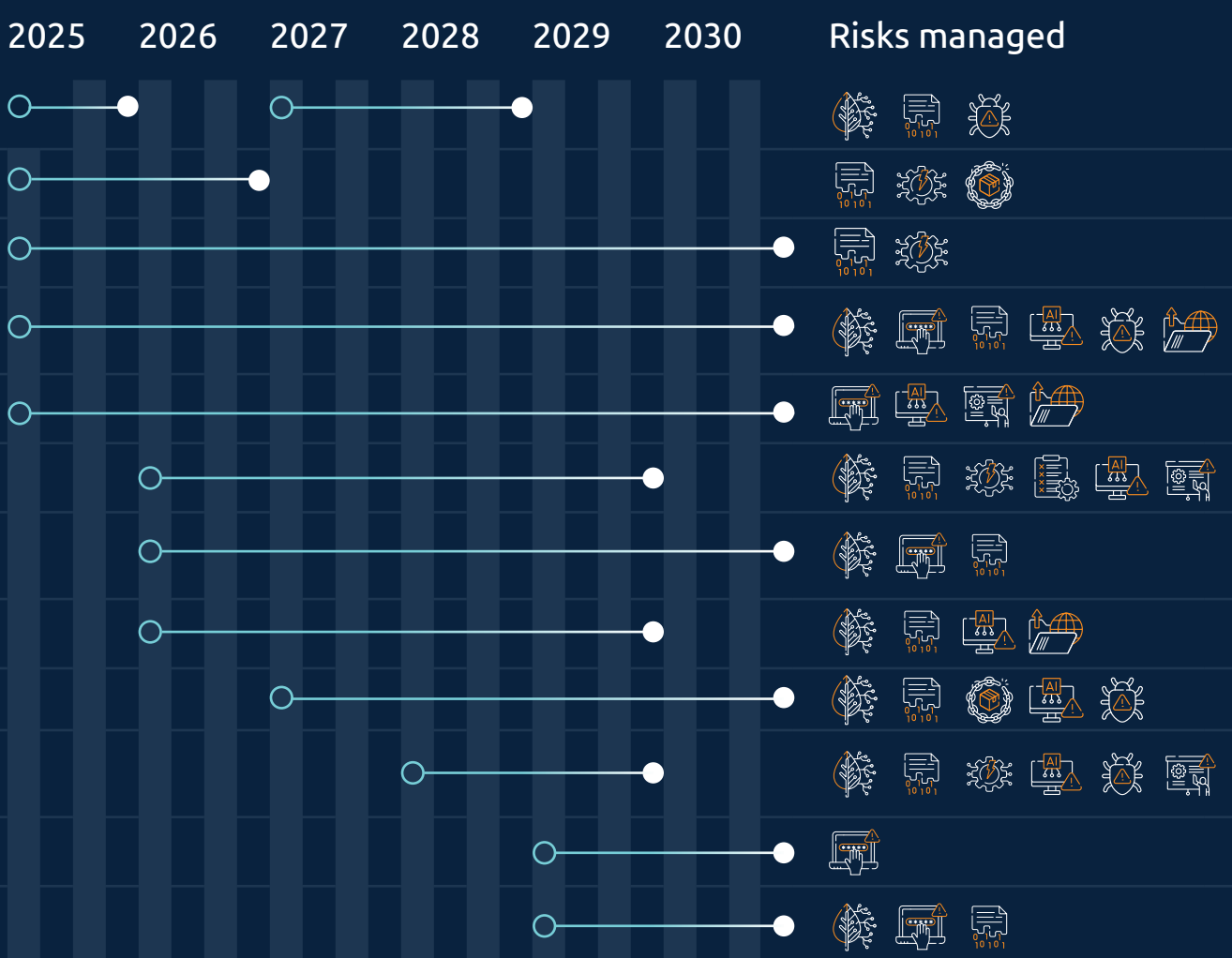
Loss, abuse or misuse of credentials

Loss of sensitive data

When

2029–2030

Roadmap


Key initiatives
2025
2026
2027
2028
2029
2030
Risks managed
1. Uplift tool of trade devices
2. Increase third-party security monitoring
3. Build resiliency into everyday operations
4. Continuously optimise cyber security operations
5. Cultivate a proactive cyber security culture
6. Embed security in operational technology
7. Introduce security measures for non-SA Power Networks devices
8. Strengthen information protection
9. Enhance identity and access controls
10. Manage risk across the software development lifecycle
11. Centralise identity management
12. Introduce network detection and response capabilities

Measuring our success

Success is being able to keep South Australia safe and empowered

The Cyber Security Strategy 2025–2030 represents the culmination of several years' work to understand, forecast, prepare for and manage safe and secure electricity supply for South Australia for the next five years, and beyond. It contributes to the achievement of SA Power Networks Digital and Data Strategy and will guide our work in this crucial space.

Our fulfilment of the actions detailed for each of the 12 key initiatives in the strategy will be delivered within the context of SA Power Networks internal and external cyber security governance and compliance regulations.

Externally, we work hard to maintain our existing levels of compliance with the AESCSF – a cyber security framework specifically designed for the Australian energy sector. Its purpose is to empower participants to assess and improve their cyber security capabilities and maturity. Participating in AESCSF provides numerous benefits for the SA Power Networks Group. It helps us have an informed view of our cyber security priorities and investments, which we use to drive our security program. We will continue to prioritise participating in AESCSF.

Internally, we will establish a metrics framework for each key initiative that includes qualitative and quantitative metrics, to evaluate the effectiveness of the actions embedded within, and to support progress reporting.

We will report regularly against the initiatives, individually and as a whole, to internal stakeholders and in our annual cyber security reports. These are publicly available – read our latest Cyber Security Annual Report.

Monitoring and managing these threats and critiquing and optimising the robustness of our initiatives is an ongoing focus for SA Power Networks as we do the vital work of empowering South Australia. At the same time as implementing the Cyber Security Strategy 2025–2030, we will conduct regular and ongoing cyber security operations to ensure the maintenance and uplift of SA Power Networks network security.

This strategy is essential to SA Power Networks overall mission. We will harness our values – we keep everyone safe; we collaborate with purpose; we take the initiative; we rise to the challenge – as we do this vital work to keep South Australia safe and empowered now, and into the future.

The illuminated Adelaide city skyline at night, seen from the Adelaide Hills.

SOCIALLY™
INCLUSIVE
DESIGN

blendcreative.com.au