Jemena Electricity Networks (Vic) Ltd

Upgrade ZSS Locks & Security Systems

Business Case

An appropriate citation for this paper is:

Upgrade ZSS Locks & Security Systems

Contact Person

Darren Ringin
Digital Project Manager
Ph: 03 9173-7000
darren.ringin@jemena.com.au

Jemena Electricity Networks (Vic) Ltd

ABN 82 064 651 083
Level 16, 567 Collins Street
Melbourne VIC 3000

Postal Address

PO Box 16182
Melbourne VIC 3000
Ph: (03) 9713 7000
Fax: (03) 9173 7516

Table of contents

List of tables

List of figures

List of appendices

1. Executive Summary

Synopsis

The purpose of this Program of works of site security system upgrades at Jemena Electricity Networks (Vic), Ltd. (JEN) zone substations is to manage risks in accordance with SGSP (Australia) Assets Pty Ltd (SGSPAA) Critical Infrastructure Risk Management Plan (CIRMP); protect our staff, systems and assets from uncontrolled access; as well as meeting *Security of Critical Infrastructure Act 2018* (SOCI Act) legislation and supporting Regulations. Sixteen (16) Zone Substations have been identified to be included in this work program.

The recommended option is to implement Jemena's site security systems that have been implemented at the JEN Tullamarine and Broadmeadows Field Depots. This will include integrating the systems into Jemena's centralised Physical site security systems, as well as the Alarm Response Management services by Jemena's 24x7 Security Monitoring Centre (SMC).

The Program is planned to commence in 2026, commissioning sites as the systems are installed, with the final site by 2031, at an estimated cost of $10.696m.

1.1 Business need

Jemena Electricity Networks (Vic), Ltd. (JEN) distributes electricity to over 370,000 customers via approximately 6,800km of distribution system and over 950 square kilometres of north-west greater Melbourne. The distribution system consists of 35 zone substations that receive sub-transmission voltages and transform this voltage to lower voltages for delivery to homes and businesses.

The SGSP (Australia) Assets Pty Ltd (SGSPAA) 'Critical Infrastructure Risk Management Plan (CIRMP) JAA LEG PR 004' describe the operational context of critical infrastructure assets (CI assets) owned and operated by SGSPAA and the material risks associated to these CI assets in line with the Security of Critical Infrastructure Act 2018 (SOCI Act).

This CIRMP supports SGSPAA to identify, and as far as is reasonably practicable, minimise or eliminate material risks that could impact the CI assets. These risks could come from any hazard, including cyber, personnel, natural disasters and supply chain.

JEN's zone substations are identified as CI assets and are to meet the requirements of SGSPAA's CIRMP.

The existing security measures at JEN's zone substations rely heavily on perimeter fencing and padlock-and-key systems which are now antiquated and inadequate for managing modern security risks to CI assets.

To manage risks in accordance with SGSPAA's CIRMP and comply with the SOCI Act legislation and supporting Regulations,[1] JEN must uplift the physical protection of it's CI assets as far as it is reasonably practicable to do so.

JEN considers it is reasonably practicable to undertake this Program to upgrade the security systems at the zone substations for Access Control, Video Surveillance and Alarm Response Management, which addresses the above by introducing auditable access control and robust response mechanisms to mitigate risks to CI assets as listed in SGSPAA's CIRMP.

Table 1 below summarises the risks logged in Omnia (SGSPAA's governance, risk and compliance system) and associated with existing site access control and monitoring systems at zone substation sites.

[1] *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules 2023*, Section 11.

Table 1: Risks summary

Risk No.	Risk ID	Risk description
1	1017168	Potential for impact on supply reliability
2	1064682	Interference with critical IT / OT system (including SCADA) impacting JEN asset availability, reliability and integrity
3	1064021	Disruption to Control Room operations
4	1064690	Damage or compromise to AMI meters resulting in a mass disconnection of customers in JEN
5	1062713	Disruption to fault response on JEN (critical activity within ZPS South)
6	1027094	Unauthorised access at zone substations

The following options addressing these issues have been considered:

- Option 1: Do nothing.
- Option 2: Install Site Access Control at 16 sites.
- Option 3: Install Site Access Control and Video Surveillance at 16 sites.
- Option 4: Install Site Access Control and Video Surveillance at all 35 sites.

1.2 Recommendation

To manage risks in accordance with SGSPAA's CIRMP and comply with the SOCI Act legislation contained within Part 2A of the Act, it is recommended to implement Option 3. This option involves installing Jemena's security systems at 16 zone substations and will include integrating these systems into Jemena's corporate centralised 24x7 security systems. This option is recommended as it addresses the risks associated with the safety and security of staff working at the sites, and the risks associated with the protection of assets.

The security systems consists of:

- Security Access Control system;
- Security Video Surveillance system and cameras;
- Digital Corporate Network connection to integrate the above systems into the Jemena corporate centralised security systems; and
- Access control, alarm management and monitoring services by Jemena's 24 x 7 Security Monitoring Centre (SMC) to manage site access, monitor and action events / alarms generated from the security systems.

The total cost of this option is outlined in section 1.4, and totals $10.696M. This preferred solution is proposed to commence in 2026, commissioning sites as the systems are installed, with the final site commissioning in 2031.

1.3 Regulatory considerations

The purpose of the SOCI Act is to provide a framework for managing risks relating to critical infrastructure by facilitating cooperation and collaboration between all levels of government, and regulators, owners and operators of critical infrastructure, in order to identify and manage those risks. As such, it requires responsible entities for

CI assets to identify and manage risks relating to those assets. JEN is bound by the SOCI Act as it is classified as a critical electricity asset.[2]

The occurrence of serious incidents at zone substation sites due to the risks and issues discussed above increase the incidence of materials risks and of JEN breaching its obligations under the SOCI Act. The objective of the project is to manage risks by upgrading the site access control and monitoring systems at nominated JEN zone substations, and to ensure continued good asset management. JEN's investment decisions are ultimately guided by the National Electricity Objective (**NEO**). Additionally, JEN is required to meet the requirements of the National Electricity Rules (**NER**), Victorian Electricity Distribution Code of Practice (**EDCoP**), and public and industry expectations for distribution system performance, which require capital expenditure objectives to be achieved as outlined in Section 2.3.

1.4 Financial information

1.4.1 Forecast expenditure and budget summary

This recommended solution proposes a total investment of $10.696M.

This project is required to be fully commissioned by 2031. Table 2 below provides the project budget by calendar year.

Table 2: Project Budget by Year[3]

Financial Year	Budget ($M)
2026-27	$1.337
2027-28	$2.005
2028-29	$2.005
2029-30	$2.674
2030-31	$2.674
Total Budget	**$10.696**

Further expenditure details are provided in section 5.

The financial evaluation is provided below.

Table 3: Financial Analysis Results Summary

Recommended option	($M)
Total Project Cost:	$10.696
NPV of Net Financial Benefit:	n/a

The project's implementation is not driven by the maximum net financial benefit returned rather the most efficient cost required to adequately and efficiently comply with JEN's SOCI Act obligations.

2 Section 10(1) of the SOCI Act.

3 Refer to attachment 'Upgrade ZSS Locks & Security Systems Costs and Benefits Analysis' for detailed calculations.

2. Background

This section sets out the case for the Program of site security system upgrades at sixteen (16) JEN zone substations, as part of JEN's EDPR 2026-2031 submission**.**

The existing security measures at JEN's zone substations rely heavily on perimeter fencing and padlock-and-key systems. While these controls may have been sufficient historically, they are now antiquated and inadequate for managing modern security risks to CI assets.

1. Fence and Padlock Systems:

   - Existing fences provide a passive barrier but are vulnerable to cutting, climbing, or other breaches; and
   - Padlock-and-key systems offer minimal control or traceability, relying on outdated manual logs and protocols that are inefficient and ineffective for managing personnel changes or addressing lost keys. The existing master key system is no longer fit for purpose; its outdated design limits security effectiveness, and replacing it would incur significant costs without delivering meaningful improvements or enhanced security outcomes.

2. Lack of Real-Time Detection:

   - Current systems do not include monitored surveillance or intrusion detection, leaving assets vulnerable to undetected breaches until routine inspections.

To address these deficiencies, JEN proposes the implementation of a comprehensive, layered security framework for the sixteen (16) zone substations. Key enhancements include:

1. Perimeter Security:

[redacted]

2. Access Control:

[redacted]

3. Intrusion Detection and Surveillance:

[redacted]

4. Lighting and Signage:

[redacted]

5. Procedural Controls:

- Regular testing of systems to ensure ongoing functionality; and
- Training for staff on new access protocols and incident response procedures.

The purpose of the Program is to manage risks in accordance with SGSPAA's CIRMP and to comply with the SOCI Act legislation and supporting Regulations. An assessment of JEN's critical infrastructure Zone Substation assets completed though SGSPAA's CIRMP has identified that these assets face material physical and personnel security hazards, which if not addressed will have a substantial impact on the assets in terms of their availability, reliability and integrity. The hazard vectors identified in the CIRMP are physical, natural and personnel; and the existing controls in place need to be upgraded to mitigate them.

Further detail on how SGSPAA's CIRMP has been used to identify the need for the upgrades and the methodology used to select the sixteen (16) critical infrastructure zone substation assets can be found in section 3.

The sixteen (16) zone substations have been selected on the basis of number of customers and [redacted] Refer to Section 3.5 for further detail.

2.1 Overview of critical infrastructure Zone Substation equipment upgrades

The site security systems to be installed create a secure working environment during and outside of business hours. The proposed solution provides the capability to manage and control site access and consists of a wide array of alarm detection devices to alert the SMC in the event of security breaches. Table 2-1 details the systems components:

Table 4: Site security systems and components[4]

System	Components
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[4] Refer to Attachment 'Site Security systems overview information – April 2024' for equipment overview.

System	Components
	[redacted]

Site security systems are to be transitioned into :

- the 24 x 7 SMC for access control, alarm management and monitoring services; and
- the Site Security Vendor Operational Maintenance Agreement.

2.2 Consumer engagement

All in-scope zone substations are located in the Melbourne and broader Metropolitan area, in suburban and industrial locations, serving both residential and commercial customers.

Jemena actively engages with emergency services, local councils, and customers to ensure alignment with community needs and resilience objectives. One key avenue for this collaboration is participation in council-led emergency management planning sessions, including the **Council Emergency Risk Assessment (CERA) process and Sector Resilience Planning (SRP)**.

The CERA & SRP process allows Jemena to:

- Understand Local, Regional and State Risk Profiles: Collaborate with councils, customers, other energy sector partners and emergency services to assess and prioritise risks impacting critical infrastructure and community safety.
- Align Mitigation Strategies: Ensure that proposed security measures address risks identified through the CERA & SRP process, reinforcing community-wide resilience.
- Foster Transparency and Trust: Share insights into Jemena's infrastructure security plans, demonstrating a commitment to protecting essential services while incorporating community feedback.

Through these engagements, Jemena ensures that its security upgrades not only comply with regulatory requirements but also integrate into broader emergency management frameworks within Victoria. This collaboration supports a unified approach to safeguarding critical infrastructure and the communities it serves.

2.2.1 Overview of consumer sentiment and relationship to this business case

Following an extensive customer engagement program[5] with residential customers, small and medium businesses and large commercial customers located within the JEN Network, we received strong feedback that customers want to ensure our assets are maintained and upgraded to ensure a safe, and reliable electricity network. In terms of our overarching customer engagement program, customer feedback on the Draft Plan highlighted that our consumer engagement has met or exceeded expectations.[6]

Over 150 residential customers from across the JEN Network provided feedback on how we can prepare our network for a more sustainable energy future while meeting customer and community needs today. When asked for feedback on priority areas for consideration by JEN, customers placed a high degree of importance on network resilience, and adopting best available technology for instantly being able to respond to shocks – which in this instance JEN considers to be the security risks of critical infrastructure. JEN considers that our obligations under the SOCI Act contribute to improving network resilience, and minimise the potential for any impacts on customers.

[5] Refer to Attachments JEN – Att 02-01 – Engagement Strategy – 20230601 – Public; JEN – Mosaic Lab Att 02-22 – Customer deep Dive outcomes report – 20241209 – Public; JEN – Sagacity Research Att 02-08 Customer priorities research report – 20241308 – Public.

[6] Refer to Attachment JEN – Att 02-18 Draft Plan Feedback Report - 20240924.

2.2.2 Jemena's People Panel

The People's Panel, a Citizen's Jury made of up to 50 residential customers, also provided a recommendation for JEN to focus on Network Resilience, to improve the networks ability to withstand and recover from hazards and disasters.

One of the People's Panel rationales for this recommendation was that it is important to invest in network infrastructure with a focus on minimising impacts on customers. Implementing site security upgrades for high priority zone substations will minimise customer impacts, through protecting our staff, systems and assets from physical risks,

For context, the People's Panel is an iterative consultation mechanism which was formed to represent customers from across JEN's network and to help us understand how we can prepare for a sustainable energy future, while meeting customer and community needs today. The People's Panel is a diverse selection of JEN's customers, incorporating all walks of life - cultural diversity, age, gender and geographic location. For reference, the People's Panel spent five Saturdays together over six months, learning about the role we play in the electricity supply network.

The alignment of our consumer engagement program with AER expectations has been detailed further in our broader regulatory proposal.

2.2.3 Engagement with Emergency Services and Customers

Jemena actively engages with emergency services, local councils, and customers to ensure alignment with community needs and resilience objectives. One key avenue for this collaboration is participation in council-led emergency management planning sessions, including the Council Emergency Risk Assessment (CERA) process and Sector Resilience Planning (SRP).

The CERA & SRP process allows Jemena to:

- Understand Local, Regional and State Risk Profiles: Collaborate with councils, customers, other energy sector partners and emergency services to assess and prioritise risks impacting critical infrastructure and community safety;
- Align Mitigation Strategies: Ensure that proposed security measures address risks identified through the CERA & SRP process, reinforcing community-wide resilience; and
- Foster Transparency and Trust: Share insights into Jemena's infrastructure security plans, demonstrating a commitment to protecting essential services while incorporating community feedback.

Through these engagements, Jemena ensures that its security upgrades not only comply with regulatory requirements but also integrate into broader emergency management frameworks within Victoria. This collaboration supports a unified approach to safeguarding critical infrastructure and the communities it serves.

2.2.4 Privacy

JEN intends to use video surveillance within the JEN zone substation sites. Video surveillance camera views will be assessed where they protrude across neighbouring properties and the use of privacy screens will be applied, as well as the provision of clear CCTV usage warning signs. JEN will undertake community consultation on privacy-related matters where appropriate, once the scope of works is formalised at each zone substation.

2.3 Regulatory and National Framework and Standards considerations

To manage risks in accordance with SGSPAA's CIRMP and comply with the SOCI Act legislation and supporting Regulations JEN must uplift the physical protection of it's CI assets as far as it is reasonably practicable to do so.

2.3.1 National Energy Rules (NER) requirements

JEN's investment decisions are guided by the NEO. Additionally, the capital expenditure objectives set out in the NER (clause 6.5.7) are particularly relevant:

a) *A building block proposal must include the total forecast capital expenditure for the relevant regulatory control period which the Distribution Network Service Provider considers is required in order to achieve each of the following (the capital expenditure objectives):*

(1) *Meet or manage the expected demand for standard control services over that period*

(2) *Comply with all applicable regulatory obligations or requirements associated with the provision of standard control services*

(3) *To the extent that there is no applicable regulatory obligation or requirement in relation to:*

(i) *The quality, reliability or security of supply of standard control services; or*

(ii) *The reliability or security of the distribution system through the supply of standard control services,*

to the relevant extent:

(iii) *Maintain the quality, reliability and security of supply of standard control services*

(iv) *Maintain the reliability and security of the distribution system through the supply of standard control services.*

(4) *Maintain the safety of the distribution system through the supply of standard control services.* [7]

Additionally, the Victorian EDCoP sets out provisions relevant to JEN's planning, design, maintenance, and operation of its network, most notably section 19.2 (Good Asset Management) and section 13.3 (Reliability of Supply):

Section 19.2 – Good Asset Management

A distributor must use best endeavours to:

a) *Assess and record the nature, location, condition and performance of its distribution system assets*

b) *Develop and implement plans for the acquisition, creation, maintenance, operation, refurbishment, repair and disposal of its distribution system assets and plans for the establishment and augmentation of transmission connections:*

- *To comply with the laws and other performance obligations which apply to the provision of distribution services including those contained in this Code*
- *To minimise the risks associated with the failure or reduced performance of assets*
- *In a way which minimises costs to customers taking into account distribution losses.*

c) *Develop, test or simulate and implement contingency plans (including where relevant plans to strengthen the security of supply) to deal with events which have a low probability of occurring, but are realistic and would have a substantial impact on customers.*

Section 13.3 – Reliability of Supply

[7] NER, cll 6.5.6(a), 6.5.7(a).

A distributor must use best endeavours to meet targets determined by the AER in the current distribution determination and targets published under clause 13.2.1 and otherwise meet reasonable customer expectations of reliability of supply.

When making decisions to invest, JEN must comply with these obligations.

2.3.2 AER assessment criteria

In preparing this business case, JEN have considered and closely followed relevant AER assessment guidelines. This includes, but is not limited to, the Better Resets Guideline and Expenditure Forecast Assessment Guideline.

2.3.3 National Frameworks and Standards for Physical Security

National Guidelines for the Protective Security of Electricity Networks (ENA Doc 0015-2022)

The proposed upgrades align directly with the ENA Guidelines for the Protective Security of Electricity Networks, emphasising risk-based, layered security measures for critical infrastructure. The specific areas of alignment include:

- Risk-Based Security Controls: Jemena's prioritisation of 16 zone substations for upgrades is underpinned by comprehensive asset-level risk assessments, which are consistent with ENA's guidelines, which advocate addressing high-priority sites first. The methodology incorporates asset criticality (based on customer demand, geographical location, past security incidents, and current vulnerabilities and security intelligence (ASIO/ Victoria Police);
- Layered Security Approach: The proposed measures enhance deterrence (access control), detection (CCTV and alarm integration), and response (centralised monitoring). This aligns with ENA's recommended framework for holistic risk management, which encompasses prevention, detection, and mitigation;
- Compliance with SOCI Legislation: ENA guidelines emphasise compliance with national regulatory requirements. The proposed upgrades address SOCI Act obligations by introducing auditable access control and robust response mechanisms to mitigate risks to key critical assets, listed in our CIRMP; and
- Security Risk Management: The proposal adheres to HB 167:2006 – Security Risk Management, which outlines best practices for identifying and mitigating security risks:
    - Integration of Risk and Security Assessments: Jemena's Security Risk Assessments (SRAs) follow HB 167 methodology, evaluating vulnerabilities and applying control effectiveness ratings to prioritise improvements. These assessments ensure that each substation's unique risks are addressed with tailored measures;
    - Control Ratings and Improvements: The business case identifies key security measures—such as electronic access controls and intrusion detection—classified under HB 167's framework as critical for transforming current controls from "adequate" to "strong."; and
    - Continuous Improvement: HB 167 highlights the importance of scalable security measures. The business case proposes integrated systems that allow for future scalability and alignment with evolving security requirements.

Australian Energy Sector Cyber Security Framework (AESCSF)

The alignment with the AESCSF is achieved by addressing the intersection of physical and cyber security by having:

- Integrated Systems: The proposed systems link physical security measures (e.g., access controls and surveillance) with Jemena's centralised corporate monitoring infrastructure. This reduces the risk of physical breaches leading to potential cyber intrusions and consequences that could not be mitigated by Cyber controls alone; and

- Compliance and Resilience: By safeguarding physical assets, Jemena enhances the overall resilience of its critical infrastructure, aligning with AESCSF's objectives for protecting essential services.

2.3.4 SOCI Act requirements

The purpose of the SOCI Act is to provide a framework for managing risks relating to critical infrastructure by facilitating cooperation and collaboration between all levels of government, and regulators, owners and operators of critical infrastructure, in order to identify and manage those risks.[8] As such, it requires responsible entities for critical infrastructure assets to identify and manage risks relating to those assets.[9] JEN is bound by the SOCI Act as it is classified as a critical electricity asset as defined in Section 10(1).[10]

SOCI Act - Part 2 - Register of Critical Infrastructure Assets

Part 2 – Register of Critical Infrastructure Assets of the SOCI Act provides that reporting entities for specified critical infrastructure assets must provide operational information, and interest and control information relating to those assets to the Register of Critical Infrastructure Assets.[11] Reporting entities also have an on-going obligation to update to the Register of Critical Infrastructure if information relating to the asset changes.[12]

SOCI Act - Part 2A – Critical infrastructure risk management programs

Part 2A - Critical infrastructure risk management programs of the SOCI Act sets out that entities with one or more critical infrastructure assets must have, and comply with, a critical infrastructure risk management program[13] (CIRMP) (unless an exemption applies) and must give an annual report relating to its critical infrastructure risk management program.

Security of Critical Infrastructure (Critical infrastructure risk management program) Rules

The Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (the Rules) specifies the requirements of a CIRMP and provides details about what constitutes a hazard and material risk to be considered. JEN has taken account of the Rules when developing its CIRMP and applied its methodology when assessing the hazards and risks of its critical infrastructure assets.

Details on how JEN has complied with the SOCI Act and Rules in forming this program of work in relation to hazard identification, material risk and relevant impact, as outlined in SGSPAA's CIRMP and as they relate to the 16 zone substation sites that require security upgrades, is set out in section 3.

8 SOCI Act, Part 1, Division 1, s.3.

9 Ibid.

10 SOCI Act, Part 1, Division 2, s.10(1).

11 SOCI Act, Part 2, Division 3, s.23.

12 SOCI Act, Part 2, Division 3, s.24.

13 Defined as an Infrastructure Risk Management Program (CIRMP) in the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules.

3. Identified critical infrastructure assets and alignment with SOCI Act and Rules requirements

In developing this program of work, JEN has used its CIRMP to identify the hazard present at zone substations, determined that the risk is material and assessed that the relevant impact will affect the assets availability, reliability and integrity. Further, the CIRMP has confirmed that the program of works addresses a material risk that is not adequately managed by the current risk management controls. The remainder of this section outlines how the CIRMP has informed the need for zone substation upgrades to ensure the material risks identified are mitigated against with regard to their impact on asset availability, reliability and integrity. Development of the CIRMP and governance

In accordance with Part 2A - Critical infrastructure risk management programs of the SOCI Act, JEN has in place a CIRMP[14] for each of its critical infrastructure assets to:

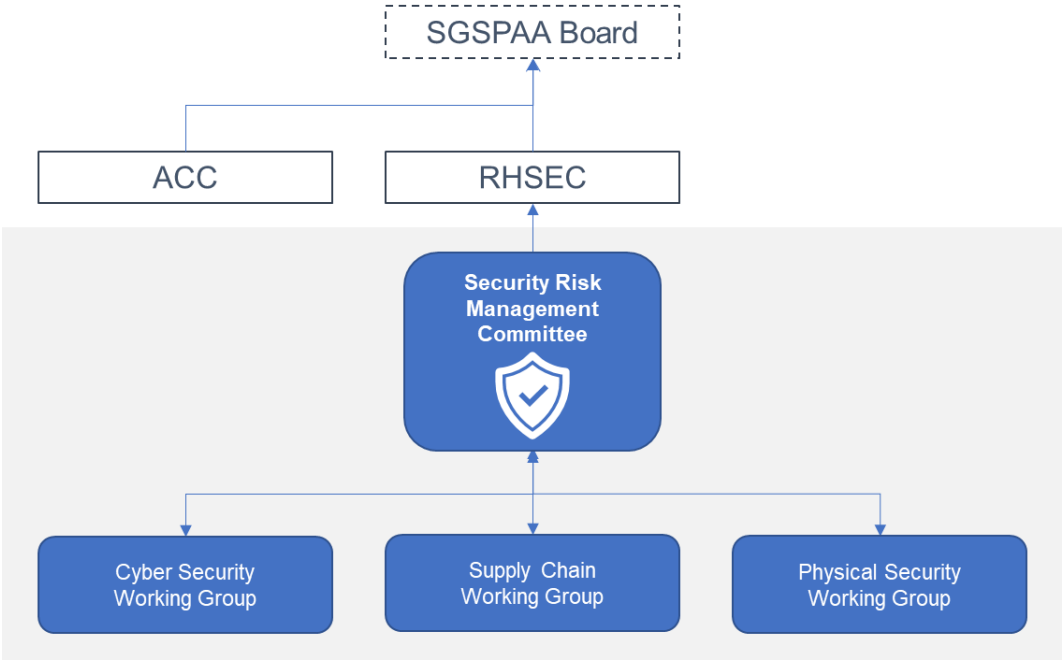
a) identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset;

b) so far as it is reasonably practicable to do so—minimise or eliminate any material risk of such a hazard occurring;

c) so far as it is reasonably practicable to do so—mitigate the relevant impact of such a hazard on the asset.

As part of the governance arrangements to ensure SGSPAA's CIRMP is conforming with the requirements of the SOCI Act and Rules, a Security Risk Management Committee (SRMC) has been formed that is responsible for developing and implementing the CIRMP. The SRMC provides oversight of CIRMP compliance, including on the hazard vectors which are set out in the Part 2A of the Rules as requiring a specific response from JEN. Figure 1 below shows the SRMC governance structure and details the key groups of the SGSPAA Board[15], the ACC[16] and the RHSEC[17].

Figure 1: Security Risk Management Committee governance structure



14 Refer to Attachment JAA LEG PR 0004 for CIRMP.

15 SGSPAA Group owns and operates the critical infrastructure assets as defined in the SOCI Act.

16 Board Audit & Compliance Committee of SGSPAA.

17 Board Risk, Health, Safety and Environment Committee of SGSPAA.

The SRMC is supported by an overall SOCI Program Working Group and working groups specific to each hazard vector (e.g. Cyber Security, Supply Chain and Personal Security) to support the delivery of SGSPAA's CIRMP objectives.

The CIRMP, along with supporting information (e.g. risk register), is reviewed and updated on an annual basis by the SRMC and in the following circumstances to ensure it is kept current:

- Changes in legislation and standards impacting JEN's critical infrastructure assets;
- Changes to operational context of critical infrastructure assets (e.g. changes in ownership due to asset acquisition or disposal); and
- Significant incidents impacting availability of JEN's critical infrastructure assets.

In accordance with Part 2 – Register of Critical Infrastructure Assets of the SOCI Act, the SRMC has identified in the CIRMP JEN's zone substations as critical infrastructure assets, as well as listing them on the Register of Critical Infrastructure Assets that is lodged with the Cyber and Infrastructure Security Centre.

3.1 Critical infrastructure asset hazard controls, identification and the CIRMP

3.1.1 Physical security controls

SGSPAA's CIRMP sets out security principles and concepts that provide a holistic and integrated protective security posture comprising physical, electronic and procedural security risk measures.

Security concepts and principles integral to minimising physical security hazards are:

- **Island sites –** robust site perimeters that allows the asset to stand alone as a secure site.
- **Security zoning –** effective separation between designated areas of the asset to restrict access as required.
- **Environmental security –** site design that promotes the key principle of crime prevention through environmental design (CPTED) to deter and delay threat activity in all **modes.**
- **Flexible and scalability –** controls are designed to accommodate significant change in threat and risk over the life of the asset, with regard to differing nature and scale that the site could be used as part of the asset's strategy.
- **Risk based approached -** utilisation of a process of Physical Security Risk Assessment (SRA) to guide JEN's security approach and mitigation at the site level. This process is detailed in SGSPAA's Group Physical Security Manual[18] and provides a transparent and consistent methodology for assessing security threats, vulnerabilities and asset criticality at specific sites and potential consequences. The SRA process also informs the development of a strategy to proportionately and cost-effectively address physical security and natural hazards risks by providing input into identification and prioritisation of potential improvements.

The CIRPM also outlines that physical security risk assessments be conducted at a minimum of every five years or when there has been a significant change to the site's use or criticality. These assessments are undertaken utilising Layered Security Principles as shown in Figure 2 below.

[18] Refer to Attachment JEM MA 0011 for Group Physical Security Manual.

Figure 2: Layered Security Principles

In addition to the security principles and concepts that guide JEN's security posture, the SRMC has implemented within the CIRMP key control measures to minimise or eliminate, as far as reasonably practicable, the physical hazards identified by JEN and defined in the SOCI Rules[19]. The controls include:

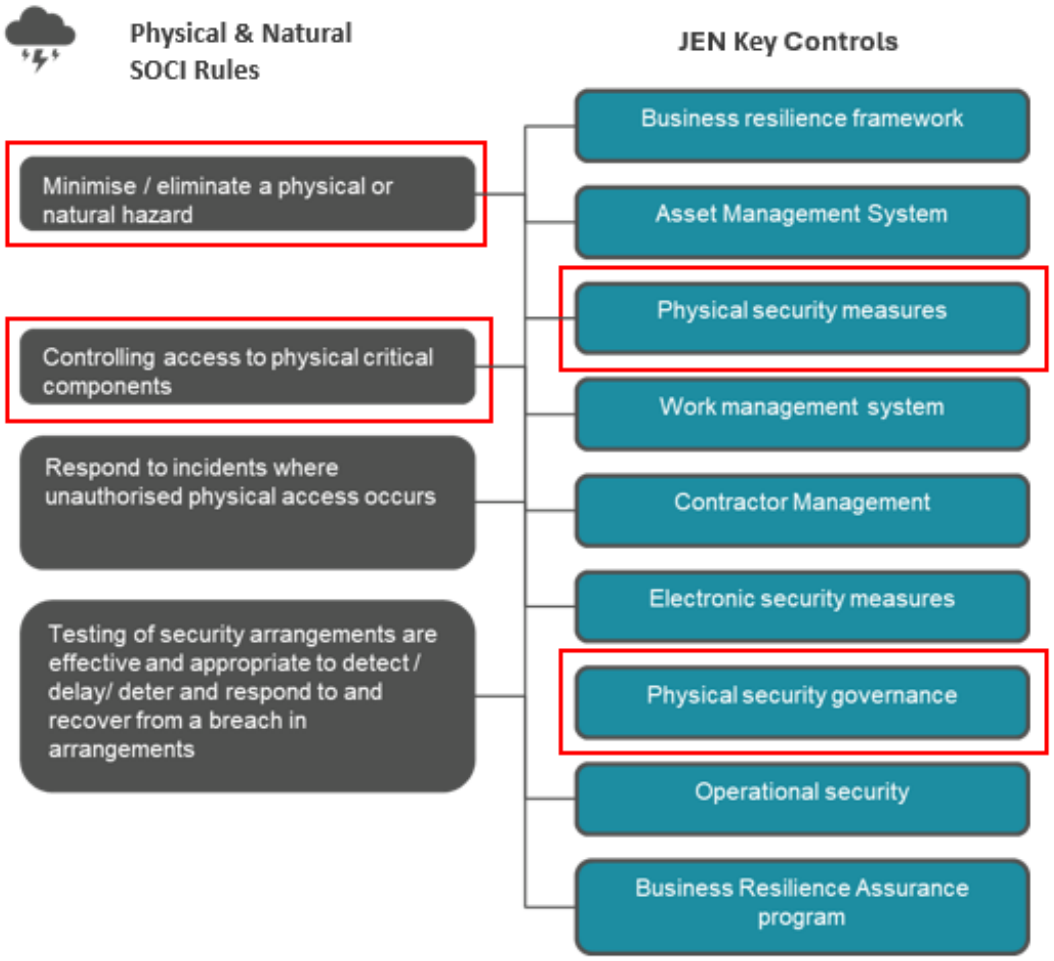
- **Physical security measures –** Physical security measures in place strengthen the exposure of our assets to sources of threat by strengthening factors such as deterrence, delay and/or denial. Includes fencing & gates, architectural elements (walls/doors), lighting, signage, lock and keying.
- **Electronic security measures –** Electronic security measures are primarily used to enhance situational awareness and detect the presence of a threat actor. They are also used for evidentiary purposes and support response, recovery and post-event review and investigation activities. These include security management systems, video surveillance (CCTV), intrusion and perimeter detection, after-hours locking systems, intercom and biometrics/2-factor authentication for higher-risk areas.
- **Physical security governance –** The effectiveness of security management frameworks and programs requires dedicated governance arrangements. Governance arrangements in place ensure clear communication through and across the roles and responsibilities undertaking physical security activities:
    - Top-down leadership provides the strategic direction and sets the performance requirements and expectations for the implementation of security arrangements; and
    - Bottom-up feedback on the performance and effectiveness of various security arrangements is necessary for strategic direction to remain relevant.

Our governance approach includes site-level Security Risk Assessment program, vulnerability assessment, security intelligence / threat context review and testing arrangements.

Figure 3 below shows the governance structure of key controls related to physical and natural hazards.

[19] SOCI Rules, Part 1, s.3.

Figure 3: Key controls related to Physical and Natural hazards



The key controls in place set out in JEN's Physical security measures, contained in the CIRMP, have identified the following components located within zone substations that are not installed, or not performing to the standard expected to maintain adherence to requirements of the SOCI Act:

Access control

Currently, there is a low level of control for gate access at these facilities.

The existing security measures at JEN's zone substations rely heavily on perimeter fencing and padlock-and-key systems. While these controls may have been sufficient historically, they are now antiquated and inadequate for managing modern security risks to CI assets.

- Fence and Padlock Systems:
    - Existing fences provide a passive barrier but are vulnerable to cutting, climbing, or other breaches.
    - Padlock-and-key systems offer minimal control or traceability, relying on outdated manual logs and protocols that are inefficient and ineffective for managing personnel changes or addressing lost keys. The existing master key system is no longer fit for purpose; its outdated design limits security effectiveness, and replacing it would incur significant costs without delivering meaningful improvements or enhanced security outcomes.
- Lack of Real-Time Detection:

- Current systems do not include monitored surveillance or intrusion detection, leaving assets vulnerable to undetected breaches until routine inspections.

Padlocks and keyed entry for perimeter and internal access ways are used to secure the site. Implementing a robust access control system with physical and digital credentials, is imperative to regulate entry and enhance security measures effectively.

Intrusion Detection

The absence of intrusion detection measures leaves the facilities vulnerable to unauthorised access. Implementing access control at site entries and intrusion detection at key site buildings, coupled with connectivity to the corporate based centralised site security systems will enable efficient control, monitoring and detection of any unauthorised entry attempts.

Video Surveillance

The introduction of surveillance capabilities will allow JEN to monitor any suspicious activities effectively. An enterprise-grade video surveillance monitoring system featuring smart cameras equipped with motion detection features would provide real-time alerts and facilitate prompt responses to potential security threats, including unauthorised operations. Full coverage of CCTV cameras ensures comprehensive intrusion detection and activity monitoring, providing a detailed understanding of site conditions.

Prevent Criminal, Malicious and Unintentional Threat

The overarching goal is to safeguard the facilities against a range of threats, including criminal activities, malicious intrusions, and unintentional breaches. By implementing robust security measures, this Program aims to mitigate risks and ensure the safety and integrity of the critical assets.

The measures in place, as noted above, to secure against physical security hazards are not currently, as far as reasonably practicable, adequate to minimise or eliminate threats identified in the CIRMP. The program of works proposed in this business case will remedy this situation.

3.1.2 Personnel security controls

SGSPAA's CIRMP sets out personnel hazard vectors related to the relevant material risks they face. Critical workers have been identified as having a material impact on the operation of critical assets and/or critical components. Criteria for identification must satisfy all three of the following conditions:

1. Is an employee or contractor (i.e. fixed term employee) with physical or cyber access including those with limited engagement including System Access Only (consultants) providers of services;

2. Their absence or compromise would prevent the proper functioning or causes damage; and

3. Has access to, control of, or management of the asset or component.

All roles have been identified against critical infrastructure assets and / or critical components and are defined in the JEN's Critical Worker Register. The register is updated on an as needed basis to capture new roles as they are created based on organisational need.

Critical staff are identified within JEN by the criteria outlined in Table 5 below.

Table 5: Critical worker identification criteria

Identification criteria	Mode	Application
Physical access	Card / key	– Proximity access to critical asset / critical components – Malicious / negligent activity on equipment, components, systems. – Includes Engineers, operators, technicians, administrators, system controllers, senior staff with authorisation responsibilities, leaders, support functions, e.g. Digital, EMT – Unescorted access to facilities and systems.
System access	Administration, user access privileges i.e. MasterSCADA, SCADA Experion, UIQ, SRTS.	– System configuration, control and administration. – Includes Engineers, operators, technicians, system administrators, system controllers senior staff with authorisation responsibilities, leaders e.g. Digital, EMT.

SGSPAA's CIRMP has identified the following components located within zone substations that are not installed, or not performing to the standard expected to maintain adherence to requirements of the SOCI Act with regard to personnel hazards:

Access control

Currently, there is a low level of control for gate access at these facilities. Padlocks and keyed entry for perimeter and internal access ways are used to secure the site.

The existing security measures at JEN's zone substations rely heavily on perimeter fencing and padlock-and-key systems. While these controls may have been sufficient historically, they are now antiquated and inadequate for managing modern security risks to CI assets.

- Fence and Padlock Systems:
    - Existing fences provide a passive barrier but are vulnerable to cutting, climbing, or other breaches.
    - Padlock-and-key systems offer minimal control or traceability, relying on outdated manual logs and protocols that are inefficient and ineffective for managing personnel changes or addressing lost keys. The existing master key system is no longer fit for purpose; its outdated design limits security effectiveness, and replacing it would incur significant costs without delivering meaningful improvements or enhanced security outcomes.
- Lack of Real-Time Detection:
    - Current systems do not include monitored surveillance or intrusion detection, leaving assets vulnerable to undetected breaches until routine inspections.

Padlocks and keyed entry for perimeter and internal access ways are used to secure the site. Implementing a robust access control system with physical and digital credentials, is imperative to regulate entry and enhance security measures effectively.

The measures in place, as noted above, to secure against personnel security hazards are not currently, as far as reasonably practicable, adequate to minimise or eliminate threats identified in the CIRMP. The program of works proposed in this business case will remedy this situation.

3.1.3 Critical infrastructure hazard identification

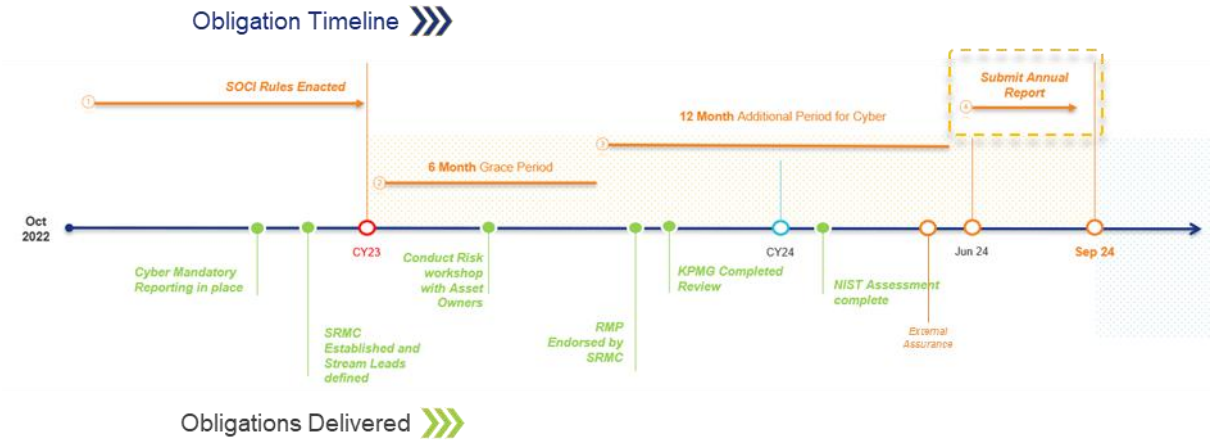
SGSPAA's CIRMP has identified all zone substations as critical assets.

3.2 Critical infrastructure asset material risk identification and the CIRMP

3.2.1 Risk criteria development

With the enactment of the SOCI Act, Jemena has developed a risk management methodology, key to which is the risk management methodology roadmap which identifies key activities, including risk assessments, to identify the risks JEN's critical infrastructure assets may be exposed to. The road map is shown in Figure 4 below.

Figure 4: Risk management methodology road map

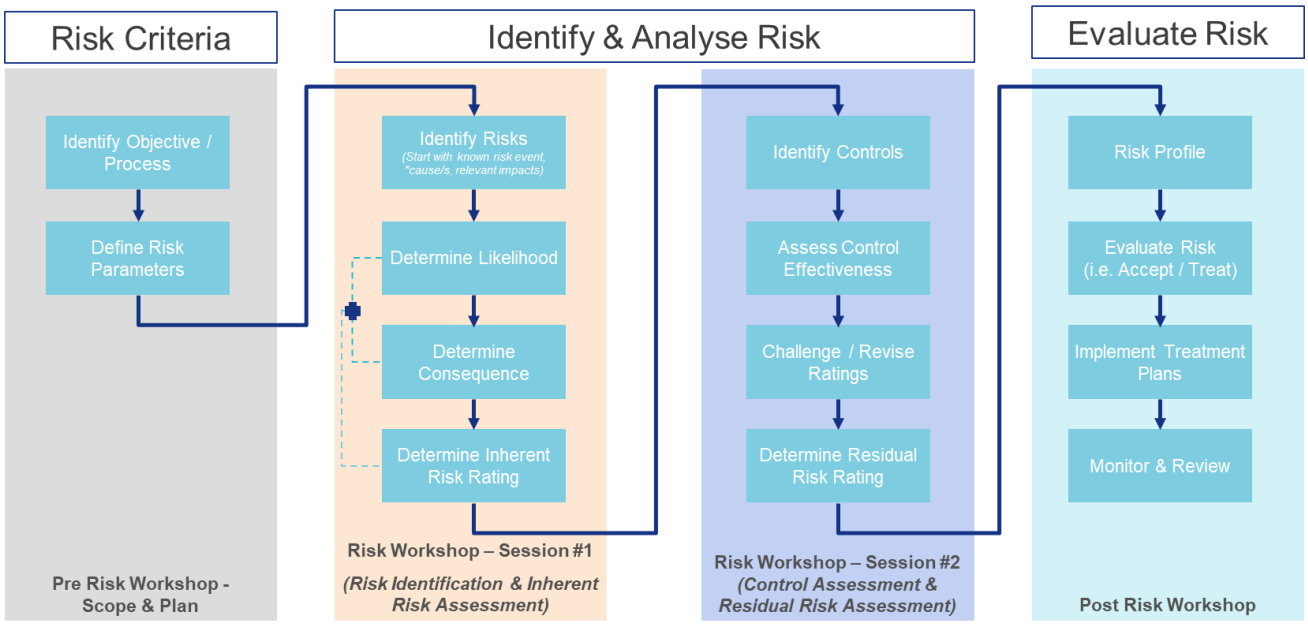


In developing the CIRMP and performing risk assessments on critical infrastructure assets, Jemena uses its risk management framework and process, having regard to the SOCI Act and Rules, risk management program guidance materials and factsheets issued by the CISC, and the operational environment in which JEN operates. The outcome of this is tailored risk criteria development was the creation of the SOCI Risk Management Guide and Asset Criticality Assessment framework The Asset Criticality Assessment guides the prioritisation of sites during the risk assessment process.

3.2.2 Risk assessment

Risk assessment activities have been completed on JEN's critical infrastructure assets following the process shown in Figure 5 below. The assessment focused on Risk Identification and Inherent Risk Assessment and Control Assessment and Residual Risk Assessment.

Figure 5: SOCI risk assessment process

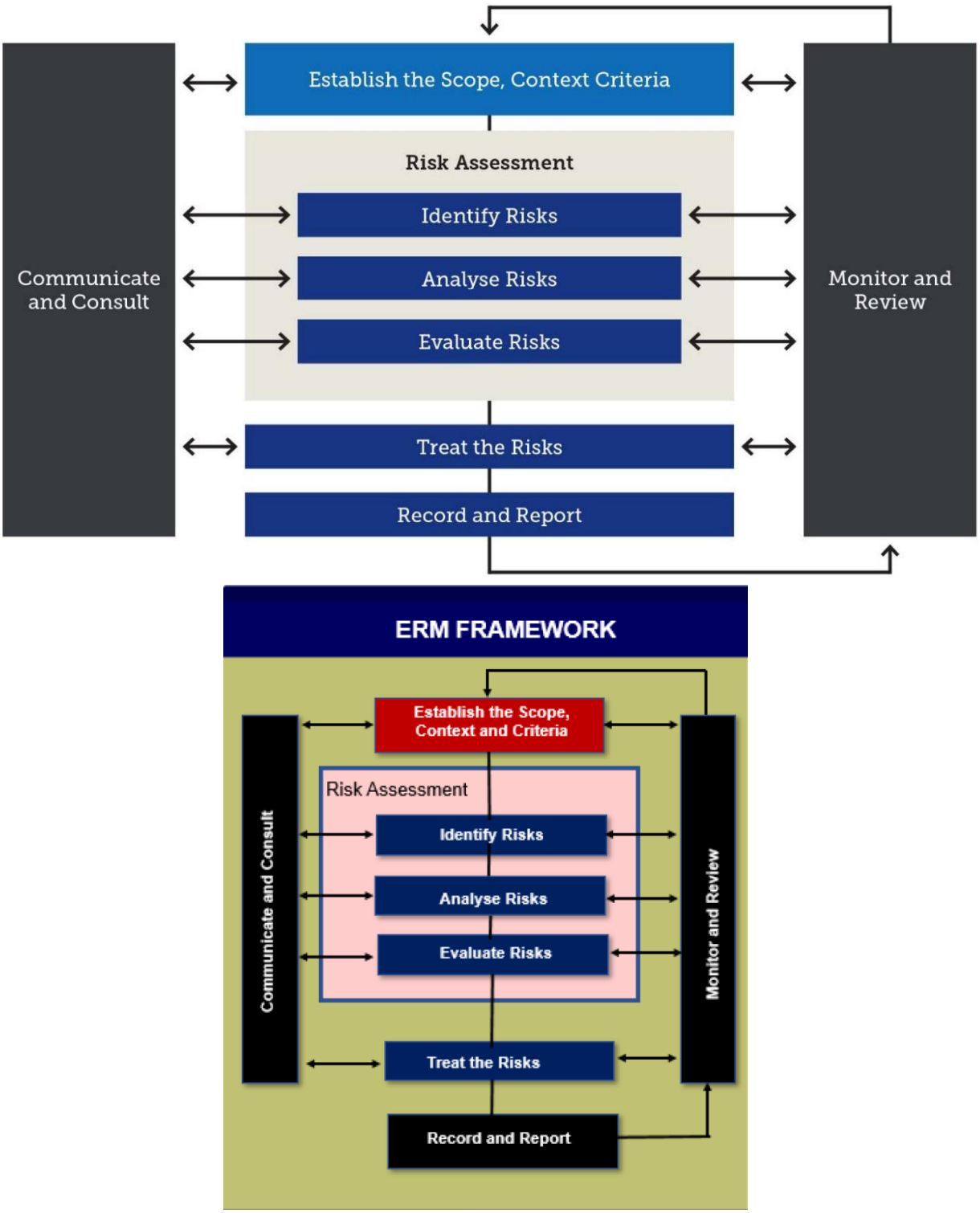


As a result of the risk assessment activities completed, a SOCI Risk Register[20] was developed which sets out information on material risks, risk causes related to the hazard vectors, applicable controls along with an assessment of control effectiveness, and risk ratings for critical infrastructure assets.

In maintaining and continually improving the CIRMP, JEN will apply its Risk Management Framework and process, as shown in Figure 6 below, for ongoing management of its SOCI material risks which is designed to assist JEN staff to integrate risk management into daily business activities to achieve the intended outcomes.

[20] Refer to Attachment SGSPAA Risk Register - Upgrade ZSS Locks & Security Systems for SOCI Risk Register.

Figure 6: SOCI risk assessment process



3.2.3 Material risk present

The outcome of the risk assessment workshops, and logged in Omnia (SGSPAA's governance, risk and compliance system) found that JEN's critical infrastructure zone substations were exposed to the below risks:

- Potential for impact on supply reliability (Risk ID 1017168)
- Interference with critical IT / OT systems (Risk ID 1064682)

- Disruption to Control Room operations (Risk ID1064021);
- Damage or compromise to AMI meters (Risk ID 1064690);
- Disruption to fault response operations (Risk ID 1062713); and
- Unauthorised access at zone substations (Risk ID 1027093).

The risks identified in the CIRMP and the risk analysis undertaken by JEN show that a material risk exists if the current physical and personnel security measure in the place at the 16 zone substations are not upgraded.

3.3 Critical infrastructure asset relevant impact identification and the CIRMP

As part of JEN's assessment of material risks contained in the CIRMP, Table 6 below identifies the relevant impacts present for JEN's zone substation critical infrastructure assets.

Table 6: Material risks overview and relevant impact

No	Material Risk	CI Asset	Relevant Impact			
		JEN	Availability	Reliability	Integrity	Confidentiality
1	Loss of supply[21]	✓	✓	✓	✓	✓
2	Interference with IT / OT system (including SCADA)	✓	✓	✓	✓	
3	Disruption to Control Room operations	✓		✓	✓	
4	Mass disconnection of AMI meters	✓	✓		✓	
5	Disruption to fault response operations	✓	✓	✓	✓	

Modelling performed by JEN shows the outcome of a material risk occurring at a zone substation will have the following effects on the networks in relation to availability, reliability and integrity:

- Loss of supply – impact due to prolonged time in restoring an outage and potential public safety incidents;
- Interference with IT / OT system (including SCADA) - impact due to disruption to Control Room operations & onsite equipment;
- Disruption to Control Room operations – impact due to prolonged time taken in restoring outage, potential public safety incidents;
- Mass disconnection of AMI meters - impact due to Loss of supply to JEN customers resulting from unauthorised disconnect; and
- Disruption to fault response operations - impact due to due to prolonged time in restoring an outage and potential public safety incidents.

[21] Risk encompasses causal factors associated with:1) damage or compromise to critical components, and 2) loss or unauthorised use of sensitive operational information (SOI).

3.4 Critical infrastructure asset incident management

In the event of an incident impacting the availability, reliability or integrity of a critical infrastructure asset, the documents set out in Table 7 below outline JEN's incident management procedure and response to be followed to ensure the integrity of the network and the safety of the public and personnel.

Table 7: Incident management procedure documents

Type of Incident	Relevant Procedure
Physical security related incidents	JAA NSO PR 0001 Alerts and Notifications Process JAA HSE PR 0004 Managing Incidents
Asset related incidents	JAA NSO PL 0003 Emergency Management Plan JAA NSO PL 0003 Annex 13 Business Continuity Plan JAA NSO PL 0002 Crisis Management Plan

Subsequent to a critical infrastructure incident, an incident investigation will be completed depending on the potential severity of the incident. The procedures to be followed are outlined in JEN's Investigate procedures framework.

The relevant impacts of the availability, reliability and integrity of critical infrastructure assets identified in the CIRMP, and the risk analysis undertaken by JEN, show that a material risk exists if the current physical and personnel security measures in the place at the 16 zone substations are not upgraded to what is proposed.

3.5 Identified zone substation critical infrastructure assets to be upgraded

The sixteen zone substations assets selected for security upgrades are listed in Table 8 below. These sites are listed on the Register of Critical Infrastructure Assets and lodged with the Cyber and Infrastructure Security Centre, and are identified in SGSPAA's CIRMP as being critical infrastructure assets. These have been identified as high priority sites to be included into this program of work based on the number of customers and supply to critical services such as e.g. Hospitals and Public Transport.

Table 8: Nominated zone substations

Site	Address	Number of Customers	Critical Services
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	Building
[redacted]	[redacted]	[redacted]	Public Transport, Major Shopping Centre
[redacted]	[redacted]	[redacted]	Healthcare and Medical
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	Public Transport, Healthcare and Medical
[redacted]	[redacted]	[redacted]	Major Shopping Centre

Site	Address	Number of Customers	Critical Services
[redacted]	[redacted]	[redacted]	Public Transport
[redacted]	[redacted]	[redacted]	Racing
[redacted]	[redacted]	[redacted]	Transport, Healthcare and Medical
[redacted]	[redacted]	[redacted]	Healthcare and Medical
[redacted]	[redacted]	[redacted]	Disaster Recovery site for JEN Control Room
[redacted]	[redacted]	[redacted]	Healthcare and Medical
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	Public Transport
[redacted]	[redacted]	[redacted]	Power Station

Note: [redacted]

4. Credible Options

This section discusses how credible options are identified and developed. The credible options are considered for their alignment to the CIRMP, commercial, technical feasibility and ability to address the identified needs, deliverability, economic and financial benefits, as well as legal and regulatory obligations.

4.1 Identifying credible options

The following feasible options could be executed to address the business need, problem or opportunity.

- Option 1: Do nothing.
- Option 2: Install Site Access Control at 16 sites.
- Option 3: Install Site Access Control and Video Surveillance at 16 sites.
- Option 4: Install Site Access Control and Video Surveillance at all 35 sites.

4.2 Developing credible options

Table 9 below shows the extent to which each option addresses the identified risks.

Table 9: Options Analysis[22]

Risk	Option 1 Do Nothing	Option 2 Install Site Access Control at 16 sites	Option 3 Install Site Access Control & Video Surveillance at 16 sites	Option 4 Install Site Access Control & Video Surveillance at all 35 sites
Risk 1 Loss of supply	◑	◑	●	●
Risk 2 Interference with IT / OT system (including SCADA)	◑	◑	●	●
Risk 3 Disruption to Control Room operations	◑	◑	●	●
Risk 4 Mass disconnection of AMI meters	◑	◑	●	●
Risk 5 Disruption to fault response operations	◑	◑	●	●

●	Fully addressed the risk
◑	Partially addressed the risk
○	Did not address the risk

[22] Refer to attachments 'Upgrade ZSS Locks & Security Systems Costs and Benefits Analysis' and 'Business Resilience MEMO JEN ZSS Security Risk Assessments February 2022' for full Cost-Benefit Analysis and Risk Assessments.

4.3 Options analysis

4.3.1 Option 1: Do nothing

In this option, no work is carried out to upgrade the security at the identified zone substations, hence existing low-level site access control is retained at the sites. All identified security, safety and reliability risks will continue as is, managed under current good asset management practices. There will be a continued threat of unauthorised access and vandalism at current levels.. Considering the significance and criticality of these sites[23] adherence to the CIRP and the SOCI Act requirements regarding the protection of critical infrastructure by owners, doing nothing is not an acceptable option.

4.3.2 Option 2: Install Site Access Control

This option proposes to replace the existing low-level site access control with access and alarm system control that can be federated into the corporate centralised systems.[24] As there is no No 24x7 video surveillance monitoring and intruder response is proposed under this option, it only partially addresses all the identified risks, aligning to the CIRMP, SOCI Act legislation and supporting Regulation.

4.3.2.1 Benefits

- Enhanced perimeter security, access control and monitoring for all site entries;
- Limited early detection: Real-time access control monitoring and alerts enable rapid response, minimising potential damage;
- Partial compliance to CIRMP and SOCI Act: Partially complies to the CIRMP and SOCI obligations under Rule 4 to minimise risks of unauthorised access and interference;
- Operational efficiency: Helps to prevents costly incidents and ensure uninterrupted service delivery to customers;
- Safety: Helps to prevents potential intrusion (malicious or opportunistic) that could lead to fatality; and
- Reduced cost involved with this option (compared with preferred option 3).

4.3.2.2 Risks

- Only covers site access control through the gates and selected doors cannot detect any other intrusion or security breaches, e.g. via fences, windows or building rooftops;
- Limited early detection: Partial real-time monitoring and alerts to enable rapid response, minimising potential damage.
- Limited resilience against advanced threats: Single system layer where the security system could be compromised by a single-point failure.

4.3.3 Option 3: Install Site Access Control and Video Surveillance

- In addition to replacing the existing low-level site access control with site access and alarm control as recommended under Option 2, this Option proposes to install 24x7 video surveillance monitoring and intruder response cameras in strategic locations around the perimeter of the sixteen (16) zone substation sites. Although more expensive then Option 2, this is the preferred option as it addresses all the identified risks, aligning to the CIRMP, SOCI Act legislation and supporting Regulations.

[23] Refer to Attachment ELE-999-PR-RM-003 JEN ASSET CRITICALITY ASSESSMENT for risk assessment.

[24] Refer to Attachment Site Security systems overview information - April 2024 for equipment overview.

.

This solution is used in recent upgrades on other SGSPAA critical infrastructure assets, [redacted]

4.3.3.1 Benefits

- Enhanced perimeter security, access control and monitoring for all site entries;
- Enhanced deterrence: Visible and robust systems discourage unauthorised attempts at entry;
- Early detection: Real-time monitoring and alerts enable rapid response, minimising potential damage;
- Resilience against advanced threats: Multiple layers ensure that the security system is not compromised by a single-point failure;
- Compliance to CIRMP and SOCI Act: Meets CIRMP and SOCI obligations under Rule 4 to minimise risks of unauthorised access and interference;
- Operational efficiency: Helps to prevents costly incidents and ensure uninterrupted service delivery to customers; and
- Safety: Prevents potential intrusion (malicious or opportunistic) that could lead to fatality.

4.3.3.2 Risks

- Longer installation timeframe due to civil works and video surveillance system; and
- May require some community consultation if CCTV camera field of views extend into neighbouring properties.

4.3.4 Option 4: Install Site Access Control and Video Surveillance across all JEN zone substation sites

This option proposes to replace the existing low-level site access control with site access and alarm control and to install 24x7 video surveillance monitoring and intruder response cameras in strategic locations around the perimeter of all sites. Although it addresses all the identified risks, aligning to the CIRMP, SOCI Act legislation and supporting Regulation, this is not the preferred options as it is more expensive than Option 3 and not the most efficient cost.

4.3.4.1 Benefits

- Enhanced perimeter security, access control and monitoring for all site entries;
- Intrusion detection and surveillance including in severe weather conditions, consistent with recent upgrades at other Jemena facilities;
- Enhanced deterrence: Visible and robust systems discourage unauthorised attempts at entry;
- Early detection: Real-time monitoring and alerts enable rapid response, minimising potential damage;
- Resilience against advanced threats: Multiple layers ensure that the security system is not compromised by a single-point failure;
- Compliance to CIRMP and SOCI Act: Meets CIRMP and SOCI obligations under Rule 4 to minimise risks of unauthorised access and interference;
- Operational efficiency: Helps to prevents costly incidents and ensure uninterrupted service delivery to customers; and

- Safety: Prevents potential intrusion (malicious or opportunistic) that could lead to fatality.

4.3.4.2 Risks

- Significantly longer installation timeframe due to volume of civil works and security systems;
- May require a larger number of community consultations if CCTV camera field of views extend into neighbouring properties; and
- Potential resourcing constrains to large Program of work.

Option 3 is the preferred option. This option resolves all identified issues while aligning with the JEN asset class and business strategies. Importantly it aligns to the CIRMP and complies to JEN's SOCI Act obligations in relation to the ownership, control and governance of critical infrastructure. The total cost of this option is outlined in Section 1.4. This preferred solution is proposed to commence in 2026, commissioning sites as the systems are installed, with the final site commissioning in 2031.

5. Option Evaluation

5.1 Economic analysis

The expected cost for each option has been captured in Table 10 below.

JEN believes Option 3 is the most prudent option to manage risks in accordance with SGSPAA's CIRMP; as well as meeting SOCI Act legislation and supporting Regulations. Therefore, it is considered the preferred option to target critical zone substation sites rather than implement works to all 35 zone substations in JEN. Table 11 below provides a summary of the cost model for this option.

Completing the works via a targeted program will ensure critical sites are prioritised and risks are mitigated in an effective manner. Design, construction and delivery efficiencies can be realised with lessons incorporated and implemented into future installations.

Table 10: Economic Analysis Results Summary

($M)	Option 1	Option 2	Option 3	Option 4
Total Expected costs	0	4.560	10.696	23.399
Option ranking	4	2	1	3

Table 11: Cost Model summary for recommended Option 3[25]

	2026-27	2027-28	2028-29	2029-30	2030-31	Total
Security systems	$674,000	$1,011,000	$1,011,000	$1,348,000	$1,348,000	$5,392,000
Civil works	$400,000	$600,000	$600,000	$800,000	$800,000	$3,200,000
Corp N/W H/W & install	$34,331	$51,497	$51,497	$68,662	$68,662	$274,649
Corp N/W service install	$14,000	$21,000	$21,000	$28,000	$28,000	$112,000
Project management	$40,000	$60,000	$60,000	$80,000	$80,000	$320,000
Site resources	$100,000	$150,000	$150,000	$200,000	$200,000	$800,000
Site management	$50,000	$75,000	$75,000	$100,000	$100,000	$400,000
Corporate network service	$16,518	$24,777	$24,777	$33,036	$33,036	$132,142
Site Security Maintenance	$8,240	$12,360	$12,360	$16,480	$16,480	$65,920
Total	**$1,337,089**	**$2,005,633**	**$2,005,633**	**$2,674,178**	**$2,674,178**	**$10,696,711**

[25] Refer to attachment Upgrade ZSS Locks & Security Systems – cost breakdown – V1.0

6. Recommendation

This business case proposes a total capital investment of $10.696m as outlined in Section Financial information1.4.

This expenditure will fulfil the objectives as outlined in Option 3. The scope of works includes further expanding the implementation of the site access control and security video surveillance system that has been implemented at the JEN Tullamarine and Broadmeadows Field Depots. This will include integrating the site security systems into Jemena's corporate centralised 24x7 security monitoring system.

This option addresses all identified risks in accordance with SGSPAA's CIRMP, through investments that are prudent and efficient, whilst meeting required SOCI Act legislation and supporting Regulations.

It is recommended that the project commence in 2026, commissioning sites as the systems are installed, with the final site commissioning in 2031.

Appendix A
Network Risk Assessment Summary

Jemena
bringing energy to life

A1. Network Risk Assessment Summary

Risk Register ZSS Site Security systems upgrades - EDPR submission 2026-2031

Participants: Darren Ringin

S/No	Business Unit	Business Objective Category	Risk type	Risk Title	Risk Description	Root Causes Category	Root Causes - Description (Contributing Factors)	Risk Consequence Category	Risk Consequence - Description	Risk Owner	Untreated Consequence	Untreated Likelihood	Untreated Risk Rating	Current Controls	Control Assessment Frequency	Control Owner	Control Effectiveness	Overall Control Effectiveness	Current Consequence	Current Likelihood	Current Risk Rating	Risk Assessment Frequency
1	Jemena Networks - Electricity	Sustainability	O-Asset & Security	Unauthorised access at zone substations (Risk ID 1027093)	Unauthorised access at zone substations Potential for unauthorised access within Jemena zone substations, resulting in trip hazards, equipment failure due to vandalism, initiation of fire and/or oil spill	Technology - New, Amended, Adopted Technology	Breach of zone substation security (i.e. damaged fences, broken locks, forced entry etc.)	Health, Safety & Environment	Major due to total permanent disability (staff or contractors), multiple hospitalizations, permanent disability and/or life-threatening injuries affected member(s) of the public	Primary Team Leader	Catastrophic	Unlikely	High	Technical Standards Install site cameras during construction period Zone substation security strategy Copper theft preventation strategy Physical barriers Asset inspection	Every 12 Months(s) never ending Every 12 Months(s) never ending Every 24 Months(s) never ending Every 12 Months(s) never ending Every 12 Months(s) never ending Every 12 Months(s) never ending	Michael Ciavarella Michael Furolo Matthew Ch'ng Nicole Walker Matthew Ch'ng Matthew Ch'ng						Every 12 Month(s) never ending
2	Jemena Networks - Electricity	Sustainability	O-Asset & Security	Potential for impact on supply reliability (Risk ID 1017168)	The risk of potential impact on supply reliability. (e.g. failure of protection systems, lack of critical asset spares, lack of network capacity, failure of plant, conductor clashing, etc.)	Technology - New, Amended, Adopted Technology	• Asset failure including deterioration of assets / age • Protection failure • Faults on the network (eg. HV conductor clashing, lighting, storms, veg) - External causes • Human error • Inaccurate demand forecasting, keeping customers on supply, unknown changes to demand • Unauthorized access / network / systems • Third party damage to assets (e.g. vehicle impact, dug ups, contacts with live conductors) • Non-Compliance to maintenance Strategies	Regulatory & Compliance	Operational / Financial / Regulatory & Compliance Loss of supply and supply reliability, regulatory scrutiny, STPIS impact Serious due to potential of loss of supply up to 3,000 customers on a feeder Likelihood: Possible due to previous occurence on the JEN network. It may occur within the next 5 years.	GM Asset & Operations - Electricity	Severe	Rare	Moderate	A suite of control activities for Cyber Security risk Maintain adequate, appropriate and comprehensive liability insurance coverage Emergency management capability Asset Management System (AMS)	Every 12 Months(s) never ending	David Worthington Phillip Stacey Fiona Dunk Brett Wilson/Michael Ciaveralla/David Spears						Every 12 Month(s) never ending
3	Jemena Networks - Electricity	Sustainability	O-Asset & Security	Disruption to control room operations (Risk ID1064021)	Disruption to JEN control room operations	Technology - New, Amended, Adopted Technology	• Loss of critical worker or personnel due to industrial actions, pandemic, high staff turnover etc. • Loss of key facilities or buildings due to fire, natural disaster etc. • Loss of IT/OT systems (e.g. SCADA) due to cyber attack, comms outage etc.	Operational	Impact on JEN availability, reliability & integrity Prolonged time taken in restoring outage, potential public safety incidents	Network Assets Manager	Major	Possible	High	Digital Management (DM) Business Resilience Framework (BRF) Industrial Relations / Workplace Relations Strategy Group Business Continuity Plan Background checks Electronic security measures	Every 12 Months(s) never ending Every 6 Months(s) never ending Every 12 Months(s) never ending Every 12 Months(s) never ending Every 6 Months(s) never ending Every 6 Months(s) never ending	David Worthington Fiona Dunk Ian Carter Emma Peck Mark Gorodecki Andrew Haigh						Every 12 Month(s) never ending
4	Jemena Networks - Electricity	Sustainability	Regulatory risk	Interference with critical IT / OT systems (Risk ID 1064682)	Interference with critical IT / OT system (including SCADA) impacting JEN asset availability, reliability and integrity	Technology - New, Amended, Adopted Technology		Operational		Network Assets Manager	Catastrophic	Possible	Extreme	Digital Management (DM) Business Resilience Framework (BRF) Background checks	Every 12 Months(s) never ending Every 6 Months(s) never ending Every 6 Months(s) never ending	David Worthington Fiona Dunk Mark Gorodecki						Every 12 Month(s) never ending
5	Jemena Networks - Electricity	Sustainability		Damage or compromise to AMI meters (Risk ID 1064690)	Damage or compromise to AMI meters resulting in a mass disconnection of customers in JEN	Technology - New, Amended, Adopted Technology	Cyber threats - unauthorised access to network / software	Operational	Loss of supply to JEN customers resulting from unauthorised disconnect	Network Assets Manager	Catastrophic	Possible	Extreme	Digital Management (DM) Business Resilience Framework (BRF) Background checks	Every 12 Months(s) never ending Every 6 Months(s) never ending Every 6 Months(s) never ending	David Worthington Fiona Dunk Mark Gorodecki						Every 12 Month(s) never ending

Appendix B
Cost Breakdown

Jemena
bringing energy to life

B1. Cost Breakdown

Upgrade ZSS Locks & Security Systems

Sites $ calcs - both Access Ctl & VMS

Size	Security systems	Civil works	Corp network H/W & install	Corp N/W service install (NBN)	Project management	Site resources	Site management	Corporate network service	Security systems maintenance	Total
All - 2026-27	$337,000	$200,000	$17,166	$7,000	$20,000	$50,000	$25,000	$8,259	$4,120	$668,544
All - 2027-28	$337,000	$200,000	$17,166	$7,000	$20,000	$50,000	$25,000	$8,259	$4,120	$668,544
All - 2028-29	$337,000	$200,000	$17,166	$7,000	$20,000	$50,000	$25,000	$8,259	$4,120	$668,544
All - 2029-30	$337,000	$200,000	$17,166	$7,000	$20,000	$50,000	$25,000	$8,259	$4,120	$668,544
All - 2030-31	$337,000	$200,000	$17,166	$7,000	$20,000	$50,000	$25,000	$8,259	$4,120	$668,544

EDPR estimates		Calculation check	Should total	Actual total	Difference
Total EDPR Sites	16	16 sites	$10,696,711	$10,696,711	$0

Financial years and sites						
Sites	Year ->	2026-27	2027-28	2028-29	2029-30	2030-31	Total
16		2	3	3	4	4	16

Costs - CAPEX	2026-27	2027-28	2028-29	2029-30	2030-31	Total	
Security systems	$674,000	$1,011,000	$1,011,000	$1,348,000	$1,348,000	$5,392,000	
Civil works	$400,000	$600,000	$600,000	$800,000	$800,000	$3,200,000	
Corp network H/W & install	$34,331	$51,497	$51,497	$68,662	$68,662	$274,649	
Corp N/W service install (NBN)	$14,000	$21,000	$21,000	$28,000	$28,000	$112,000	
Project management	$40,000	$60,000	$60,000	$80,000	$80,000	$320,000	
Site resources	$100,000	$150,000	$150,000	$200,000	$200,000	$800,000	
Site management	$50,000	$75,000	$75,000	$100,000	$100,000	$400,000	
Corporate network service	$16,518	$24,777	$24,777	$33,036	$33,036	**$132,142**	
Security systems maintenance	$8,240	$12,360	$12,360	$16,480	$16,480	**$65,920**	
Total	**$1,337,089**	**$2,005,633**	**$2,005,633**	**$2,674,178**	**$2,674,178**	**$10,696,711**	**2024 $**

Sites $ calcs - Access Ctl only

Size	Security systems	Civil works	Corp network H/W & install	Corp N/W service install (NBN)	Project management	Site resources	Site management	Corporate network service	Security systems maintenance	Total
All - 2026-27	$100,000	$50,000	$30,000	$15,000	$15,000	$50,000	$15,000	$8,000	$2,000	$285,000
All - 2027-28	$100,000	$50,000	$30,000	$15,000	$15,000	$50,000	$15,000	$8,000	$2,000	$285,000
All - 2028-29	$100,000	$50,000	$30,000	$15,000	$15,000	$50,000	$15,000	$8,000	$2,000	$285,000
All - 2029-30	$100,000	$50,000	$30,000	$15,000	$15,000	$50,000	$15,000	$8,000	$2,000	$285,000
All - 2030-31	$100,000	$50,000	$30,000	$15,000	$15,000	$50,000	$15,000	$8,000	$2,000	$285,000

EDPR estimates		Calculation check	Should total	Actual total	Difference
Total EDPR Sites	16	16 sites	$4,560,000	$4,560,000	$0

Financial years and sites						
Sites	Year ->	2026-27	2027-28	2028-29	2029-30	2030-31	Total
16		2	3	3	4	4	16

Costs - Capex	2026-27	2027-28	2028-29	2029-30	2030-31	Total
Security systems	$200,000	$300,000	$300,000	$400,000	$400,000	$1,600,000
Civil works	$100,000	$150,000	$150,000	$200,000	$200,000	$800,000
Corp network H/W & install	$60,000	$90,000	$90,000	$120,000	$120,000	$480,000
Corp N/W service install (NBN)	$30,000	$45,000	$45,000	$60,000	$60,000	$240,000
Project management	$30,000	$45,000	$45,000	$60,000	$60,000	$240,000
Site resources	$100,000	$150,000	$150,000	$200,000	$200,000	$800,000
Site management	$30,000	$45,000	$45,000	$60,000	$60,000	$240,000
Corporate network service	$16,000.00	$24,000.00	$24,000.00	$32,000.00	$32,000.00	**$128,000**
Security systems maintenance	$4,000.00	$6,000.00	$6,000.00	$8,000.00	$8,000.00	**$32,000**
Total	**$570,000.00**	**$855,000.00**	**$855,000.00**	**$1,140,000.00**	**$1,140,000.00**	**$4,560,000**