January 2026

Powerlink 2027-32 Revenue Proposal

IT/OT Cyber Security Program Investment Case

Contents

1. Executive Summary

This investment case documents the justification for planned investment in cyber security management capability and infrastructure for Powerlink Queensland, including both Information Technology (IT) and Operational Technology (OT) requirements. It is based on the planning undertaken to date, the estimated costs and the associated risks.

Powerlink is the electricity transmission network service provider (TNSP) for Queensland, operating critical infrastructure that underpins the energy supply for the state, and for the wider east coast.

Like all modern utilities, Powerlink relies on complex IT and OT systems to run its network and business processes. Growth of the cyber security threat in the modern world is well documented. Threat actors seek to leverage organisations' dependence on information and systems for their own financial or political gain, which in turn, can disrupt customer service delivery, threaten the achievement of strategic objectives and harm business reputations.

The Australian Signal Directorate's (ASD) Australian Cyber Security Centre (ACSC) monitors Australia's cyber threat landscape and publishes an annual Cyber Threat Report. Its 2024 report states that "Operational technology systems are increasingly interconnected and can have vulnerabilities that make them an easier cyber target. Secure information and communications technology and operational technology systems are necessary to protect Australia's critical services". They go on to advise that "Critical infrastructure organisations should adopt a stance of `when' not `if' a cyber security incident will occur."[1]

Since 2020, Powerlink has delivered an on-going cyber security investment program to:

- Achieve and then maintain a level of cyber security maturity across the organisation to a board-agreed level against the Australian Energy Sector Cyber Security Framework (AESCSF).
- Mitigate known and likely cyber security risks against information assets, network, IT and OT systems and equipment within an acceptable risk tolerance.
- Identify and mitigate new threats as they emerge.
- Manage and report cyber security obligations under various regulatory and legal frameworks. E.g. the Security of Critical Infrastructure Act (SOCI) mandatory risk management program.
- Govern, monitor, co-ordinate and action new investments required to maintain the above.
- Develop and test disaster recovery and business continuity planning.

This document sets out the case and drivers for Powerlink's cyber security investments for the 2027-32 regulatory period. These investments are to ensure that Powerlink continues to address new and increasingly sophisticated cyber security threats while keeping information security related risk at a level that is commensurate with Powerlink's corporate risk appetite and in line with the government and community expectations of critical infrastructure operators.

Powerlink will continue to use a mature, AESCSF aligned Information Security Management System (ISMS) to identify and implement new security controls and practices (or enhance existing controls and practices) to manage these risks.

The investment case documents the drivers and plans for three types of cyber security investment for the coming

[1] ASD Cyber Threat Report 2023-24. Chapter 2

regulatory period:

1. Sustaining cyber security defence maturity
2. SOCI Act and Proactive Risk Mitigation
3. Managing the evolving cyber security threat

This investment case considers two options to address the investment drivers, and contrasts these options against a base case (counterfactual) scenario. I.e.:

- **Option 1 (Recommended Option)** "Prudent and Proactive Cyber Security Management"
- **Option 2 (Alternative Option)** "Cyber Security Defence Uplift and Risk Minimisation"

The Recommended Option "Prudent and Proactive Cyber Security Management" addresses all identified drivers with a prudent expenditure profile.

Note that all financial values in this paper are provided in FY27 Real Terms (pre-CAM[2]).

[2] The term "pre-CAM" indicates that the forecast cost represents the holistic Powerlink investment amount, prior to application of the Cost Allocation Method (CAM).

2. Investment Decision

2.1 Cyber Security Context

Technology and information management are essential to Powerlink's network and business operations. Like all contemporary businesses, Powerlink makes extensive use of systems and information to conduct normal business activities. Powerlink is also reliant on information management to design, build and operate its power and communications networks.

The rapid growth of the cyber security threat within Australia and around the world is well documented. Threat actors seek to leverage organisations' dependence on information and systems for their financial or political gain, which in turn, can disrupt customer service delivery, threaten the achievement of strategic objectives and harm business reputations.

Complex critical infrastructure organisations such as Powerlink present attractive targets. In the past decade, governments have become increasingly focussed on the resilience of critical infrastructure and have sought to ensure that services are protected against a wide range of threats. Prudent and efficient management of strong cyber security defences is therefore inherent in Powerlink's responsibilities to the Australian community.

Powerlink operates in a dynamic and increasingly hostile cyber threat environment. Globally, cyber attacks are growing in frequency and sophistication, with critical infrastructure operators like Powerlink becoming prime targets. The next five to seven years (2027-2032) are expected to bring escalating cyber risks, driven by both technological trends and geopolitical factors. Understanding this broader threat landscape is essential to inform Powerlink's security planning.

Key characteristics of the current and emerging threat environment are described below.

2.1.1 State-Sponsored Threats and Espionage

Nation-state actors continue to pose a serious threat to critical infrastructure. These attackers have advanced capabilities and motivations ranging from espionage to sabotage. Australia's security agencies warn that the nation faces a period of "strategic surprise and security fragility," with multiple threats converging by 2030.

Recent examples illustrate the risk. I.e. In 2024, a sophisticated state-affiliated group known as Volt Typhoon was discovered infiltrating utility networks in the United States, aiming to maintain long-term access and positioning itself to potentially disrupt operations later. Another state-affiliated group, Salt Typhoon, compromised telecommunications systems to spy on officials' communications. These incidents signal tactics that could be used against Australian critical infrastructure.

Australian authorities anticipate that cyber-enabled espionage and interference of this kind will increase over the coming decade, in step with rising geopolitical tensions. State actors are not only gathering intelligence but may also pre-position in networks to enable future disruptive attacks. E.g. Inserting malware that could trigger outages on energy grids.

The ongoing conflict in Ukraine has demonstrated how cyber sabotage can cause blackouts on power infrastructure, and similar capabilities are being developed by others. Powerlink must assume that persistent, well-resourced adversaries may try to penetrate its network to steal sensitive data or lay the groundwork for potential sabotage.

2.1.2 Cybercrime and Ransomware

Financially motivated cyber-criminals represent a constantly evolving threat. Ransomware attacks have reached epidemic levels globally, increasingly targeting essential service providers. Organised criminal gangs operate ransomware-as-a-service models, selling ready-made ransomware toolkits to affiliates who then carry out attacks. This franchising means even relatively low-skilled hackers can attempt large-scale ransomware attacks with high effectiveness. The lines between criminal and state actors are also blurring. Some regimes are known to engage directly in cybercrime as a source of state revenue, and some state-developed hacking tools have leaked to criminal groups.

For Powerlink, the cybercrime threat translates into risks of disruption (through ransomware or destructive malware) and data theft. Ransomware gangs could target Powerlink's IT systems or even OT environment, seeking extortion payments by threatening prolonged outages. Global trends indicate these attacks are growing more targeted and destructive.

Criminals have learned that hitting industrial companies' OT networks can increase pressure to pay. Similarly, during high-profile events or critical periods, victims may be more likely to pay a ransom quickly, which could represent a relevant factor with upcoming Queensland events (discussed below).

Powerlink must therefore prepare for increasingly bold and sophisticated criminal attacks, including simultaneous encryption of IT and OT systems or "double extortion" schemes where data is stolen and ransomed.

2.1.3 Hacktivism and Politically Motivated Attacks

Beyond espionage and profit, some threat actors are driven by ideology or politics. Hacktivist groups and extremist collectives have stepped up attacks on Australian networks over the past year in response to international events.

For example, international hacktivists have launched attacks on Australian public and private sector sites, using techniques including web defacements and denial-of-service to spread propaganda or retaliate for Australia's stance on geopolitical conflicts. Such attacks typically aim to embarrass or disrupt rather than breach data, but they can still consume significant defensive resources and may serve as a smokescreen for more damaging intrusions. They also surge during times of international tension.

Powerlink, as a critical infrastructure provider, could be targeted by hacktivists seeking to make a political statement or by groups tied to energy-related activist causes, or to cause public panic through misinformation.

2.1.4 Major Events Increasing Threat Likelihood

The local threat environment in Queensland is influenced by upcoming major events that will draw global attention.

In the lead-up to Brisbane hosting the 2032 Summer Olympics and Paralympics, as well as the 2027 and 2029 Rugby World Cups, there is an expectation of heightened cyber activity targeting organisations involved in hosting and infrastructure.

Historically, global sporting events have been prime targets for certain nation-states and cybercriminals. During the 2018 Winter Olympics, for example, state-sponsored hackers deployed destructive malware to disrupt the opening ceremony IT systems. Olympic organisers and partners have also faced spying and intrusions well in advance of events. Similar interest is anticipated in Queensland's Olympic preparatory phase, meaning that key service providers including Powerlink could see increased probing or attacks as the Olympics draw nearer.

Additionally, the influx of investment and complex supply chains around such events create more opportunities for cybercriminals (e.g. fraudulent procurement schemes or targeting of contractors).

Practically, Powerlink should be prepared for higher volumes of cyber attacks during the build-up and execution of these events, including potentially coordinated campaigns aimed at causing outages or reputational damage during globally watched periods.

2.1.5 Supply Chain and Zero-Day Attacks

Attackers are refining techniques to bypass traditional defences. Supply chain attacks remain a potent threat, whereby adversaries compromise a third-party vendor, software or hardware component as a stepping stone into the primary target. Powerlink relies on a network of suppliers and contractors (for IT software, field equipment, etc.), each a potential entry point if not secured.

A notorious example was the Kaseya incident (2021), where hackers breached a trusted IT service provider's software and pushed ransomware to hundreds of downstream clients. Another was the SolarWinds compromise (2020), where attackers implanted backdoors via a routine software update, affecting public and private sector networks worldwide. These incidents highlight the need for vigilance over third-party risk.

In mid-2025, security researchers and government officials uncovered a significant security risk involving out-of-band (OOB) communication networks hidden within modern solar inverters and battery storage systems. These "rogue" components (primarily including undocumented cellular modules or secret Wi-Fi radios) were found to be omitted from official product manuals and Software Bills Of Materials (SBOMs), effectively creating a persistent "backdoor" into critical energy infrastructure. According to investigative reports from Reuters and PV Magazine, these hidden channels allow devices to communicate directly with external servers, bypassing standard corporate firewalls, VPNs and monitoring tools. This discovery coincided with a major report from the cyber security firm Forescout, which detailed 46 vulnerabilities in inverters from major global manufacturers (such as Sungrow, Growatt and SMA). Experts warn that if these OOB networks are exploited by malicious actors, they could be used to remotely disable thousands of inverters simultaneously, leading to grid instability, physical damage to hardware, or widespread blackouts.[3]

Powerlink also must consider data supply chain exposures, as sensitive information shared with external partners can be targeted even if Powerlink's own systems are intact. Furthermore, attackers are increasingly using highly evasive techniques like fileless malware and novel attack vectors that evade legacy security tools. E.g. Browser-based attacks that abuse trusted web sessions, or malware embedded in memory, require advanced detection strategies. Overall, the trend is toward more stealthy threats that exploit trust, meaning Powerlink's threat surface extends beyond its own perimeter to its entire ecosystem of technology partners.

[3] Reuters (May 2025): "Hidden devices found in Chinese-made inverters in the US, reports Reuters."

PV Magazine (May 14, 2025): Detailed the discovery of rogue communication devices not listed in documentation.

Cybersecurity Dive (March 28, 2025): "Solar power gear vulnerable to remote sabotage," covering the 46 vulnerabilities found by Forescout.

The Hacker News (March 2025): Reported on the specific technical flaws in Sungrow, Growatt, and SMA products that enabled remote code execution.

iTnews (May 2025): "Rogue communication devices found in Chinese solar power inverters," discussing the risk of firewalls being circumvented remotely.

2.1.6 AI, Quantum Threats and Other Emerging Technologies

Rapid technology evolution is creating new dimensions of cyber security risk. On one hand, defenders have new tools (e.g. AI for anomaly detection), but attackers are equally empowered.

AI models can directly assist attackers, such as use of advanced language models to craft convincing phishing lures or even generate malware code. Experimental AI agents have also matched or exceeded human hackers in certain challenges. In the near future, an adversary might deploy an autonomous “hacking AI” that probes networks and adapts at machine speed. Meanwhile, security teams are leveraging AI for automated threat detection and response [redacted], for example, can help triage incidents using AI).

This AI arms race means the pace and complexity of cyber threats will increase. Powerlink should expect threats such as deepfake social engineering. E.g. Fraudulent voice or video messages directly mimicking executives or stakeholder representatives.

In November 2025, Anthropic revealed that a state-sponsored threat actor successfully manipulated Claude Code, an AI-powered coding tool, to orchestrate what is being called the first large-scale, "agentic" cyber espionage campaign. Unlike traditional hacks where AI acts merely as an advisor, this operation saw the AI autonomously executing 80-90% of tactical operations, including reconnaissance, vulnerability discovery and credential harvesting. The attackers bypassed Claude’s safety guardrails through a sophisticated jailbreak technique where they role-played as legitimate cybersecurity professionals conducting authorised penetration tests. By breaking down the attack into thousands of discrete, seemingly benign tasks via the Model Context Protocol (MCP), the hackers induced the AI to infiltrate approximately 30 global targets spanning financial institutions and government agencies, at speeds physically impossible for human teams.[4]

Another horizon threat is quantum computing. While still experimental, quantum computers in coming years threaten to break the cryptographic algorithms (RSA, ECC) protecting most secure communications. Adversaries may already be intercepting and storing encrypted data today, hoping to decrypt it once quantum capabilities mature (“harvest now, decrypt later”). The prospect of quantum attacks is driving many organisations to plan for quantum-safe encryption within five years. In the energy sector, which relies on encryption for both IT and OT communications (from VPNs to SCADA links), a shift to post-quantum cryptography is on the horizon to ensure future-proof security. Although quantum code-breaking is not yet a present threat, Powerlink’s long-term strategy must account for this by tracking standards. The US Government has mandated all systems be Quantum Encryption capable by 2035, with high-risk systems to be updated by 2030. [5]

In summary therefore, Powerlink faces a broad array of cyber threats, ranging from nation-state hackers and organised cybercriminal groups to opportunistic hacktivists, and challenges from emerging technology. The threat outlook is one of increasing complexity and severity. Attackers are more determined, using more advanced tools, and potential impacts (from prolonged power outages to sensitive data exposure) are escalating. Concurrently, new

[4] Anthropic Official Blog (Nov 13, 2025): "Disrupting the first reported AI-orchestrated cyber espionage campaign."
The Hacker News (Nov 14, 2025): "Chinese Hackers Use Anthropic's AI to Launch Automated Cyber Espionage Campaign."
CyberScoop (Dec 18, 2025): "Policymakers grapple with fallout from Chinese AI-enabled hack."

[5] National Security Agency (NSA): "Announcing the Commercial National Security Algorithm Suite 2.0," detailing the phased implementation through 2035.
White House NSM-10 (May 2022): "Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems."

technologies and regulatory pressures are reshaping the environment, requiring adaptation. This environment requires a vigilant and forward-looking cyber security strategy.

Powerlink's defensive posture and plans, are designed to counter these threats through robust risk management, investment in modern security controls, and alignment with best-practice frameworks and compliance requirements.

2.2 Investment Drivers

Consistent with the above context, in the coming regulatory control period, Powerlink will manage and address three sets of cyber security investment drivers as summarised below.

Driver 1: Sustaining Cyber Security Defence Maturity

Powerlink, as a member of the Cyber Security Industry Working Group (CSIWG), supports the management of cyber security risk consistent with the Australian Energy Sector Cyber Security Framework (AESCSF).

The AESCSF was developed in 2018 and refined in 2019 as a collaboration of energy industry and government stakeholders in response to recommendations from the Finkel Inquiry. AESCSF version 2 was released in late 2023 which included enhancements to align with current international standards and to address emerging cyber threats.

Powerlink established the Information Security Management Program (ISMP) in 2020 as structured investment program to manage cyber security risk and to uplift the organisation's cyber security defences. The ISMP's aim is to address Powerlink's requirement to manage assets consistent with industry-typical cyber security practices and to mitigate known cyber security risks within an appropriate risk profile in an environment of growing threat, national focus and community expectation.

Key functions of the ISMP are:

- **Program governance** of all Powerlink cyber security initiatives (IT and OT). These initiatives are monitored and reported into the centralised Information Security Senior Governance Group (ISSGG) through the ISMP.
- **Ongoing sustainment of the AESCSF defence level**, including document updates, embedding process changes and audit outcomes, benchmarking and coordination of external cyber security exercises.
- **Execution and coordination of Powerlink's Information Security Management System (ISMS)**, ensuring security risks are systematically assessed and mitigated in alignment with business objectives.
- **Planned Threat Risk Assessment (TRA) and remediation activities** consistent with Powerlink's risk tolerance framework.
- **Cyber Security Assurance** through evaluation, verification and continuous improvement of security controls.
- **Periodic review and uplift** of Cyber Security Incident Response and Recovery Plans.

Powerlink achieved an AESCSF [redacted] rating in November 2019 with an aggregate score of [redacted], reflecting a maturity rating between [redacted] for most cyber security practices. [redacted]

Under an AESCSF E-CAT[6] assessment, a Transmission Network Service Provider (TNSP) within the Australian energy market is classified at the top of the "HIGH" band and is therefore recommended to target the highest level of cyber security maturity under the AESCSF.

Although stated by AEMO[7] that CAT results do not indicate that an entity has obligations under or is compliant with applicable Commonwealth legislation, Powerlink does agree that these recommendations are commensurate with Powerlink's criticality within the energy system and therefore prudent to target over the long term, especially in an

[6] AEMO - Electricity Criticality Assessment Tool (E-CAT) 2022

[7] AEMO – AESCSF Framework Overview 2022, page 3

environment of growing threat as stated by the Australian Signal Directorate (ASD).

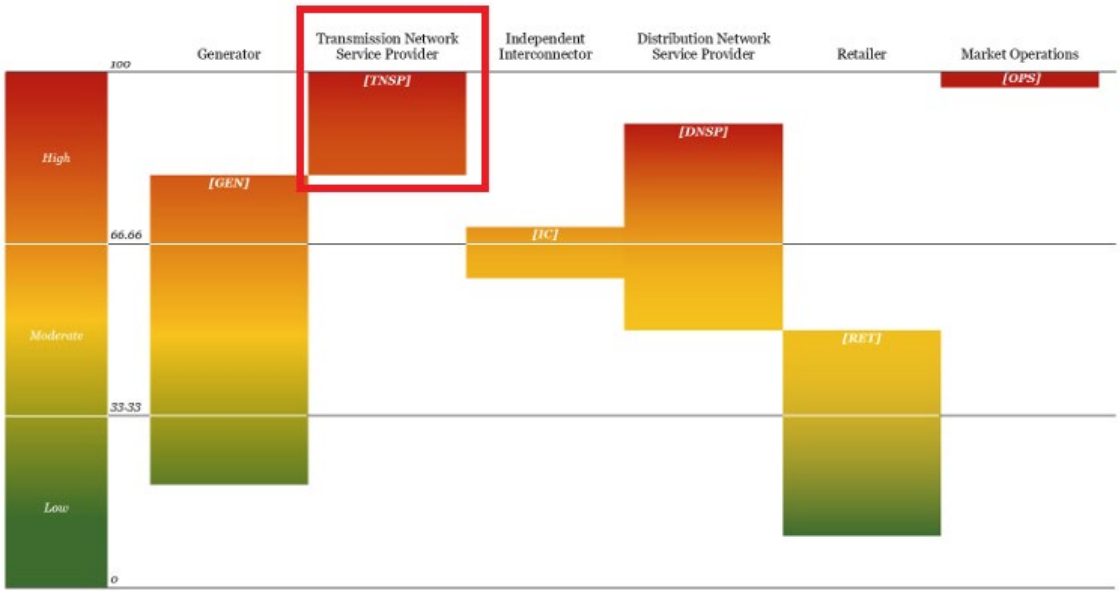


Figure 2.1- E-Cat Assessment Chart - AESCSF Guide 2022

Consistent with this, Powerlink's ISMP for the current regulatory period (2022-27) cyber security investment programs has:

- **Modernised and rationalised** existing cyber security tooling and support systems.
- Through progressive Threat Risk Assessments (TRAs) **delivered targeted investments to uplift AESCSF domains** [redacted]
- Through external assessment and threat intelligence **delivered targeted investment to manage known and emerging technical cyber security risks** in both IT and OT environments.
- **Implemented on-going cyber security awareness training** to uplift employee and supplier awareness of cyber threats.

[redacted]

In must be noted that in a rapidly changing threat landscape, especially with the advent of consumer Artificial Intelligence (AI) over the last 3 years, there is a considerable amount of investment required to maintain cyber security maturity and defences at the same level. Compensating risk controls have an increasingly shorter effective timeframe and the balance of maintaining compliance while dealing with emergent risks is a non-trivial exercise. It is also likely that the AESCSF will continue to mature, such as the AESCSF V2 release 2023 that added an additional 72 practices. To be clear "sustaining maturity" in no way translates to "do nothing".

Unless directed otherwise over the period, program investment in the 2027-32 period will concentrate on sustaining an AESCSF maturity between [redacted]

Driver 2: SOCI Act and Proactive Risk Mitigation

Complex critical infrastructure organisations such as Powerlink present an attractive target to threat actors. In the past decade, governments have become increasingly concerned with the resilience of critical infrastructure and have sought to ensure that services are protected against a wide range of threats. Since 2015, they have also particularly focussed on the management of cyber security risk.

The SOCI Act was passed by the Australian Government in July 2018 and introduced as part of the government's Cyber Security Strategy in 2020. It was amended in 2021 and 2022 to more appropriately capture those assets that are critical to Australia's defence, national security, economy and social stability. The amendments also responded to the deteriorating threat environment related to cyber-attacks.

The SOCI Act was further amended in 2024 by the Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Act 2024 (ERP Act) in response to significant incidents impacting critical infrastructure, to uplift existing obligations for affected entities and to enhance the government's ability to manage the consequences of all hazards incidents on critical infrastructure assets.

Part 2A of the SOCI Act sets out the requirement to adopt and maintain a Critical Infrastructure Risk Management Program (CIRMP). The Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023 specify the requirements of a CIRMP and provide further details of the obligations for Critical Infrastructure Providers.

The ERP Act clarifies that the protection of certain business critical data and the secondary systems that store it should be considered under the CIRMP and therefore come under the remit of SOCI reporting obligations. [redacted]

Obligations under the SOCI Act continue to evolve over time. The Australian Signals Directorate (ASD) regularly releases new guidance for critical infrastructure operators, such as the CI-Fortify guidance released in October 2025, and it is Powerlink's expectation that these guidelines, or versions of them, will become obligations over time.

Powerlink, along with other critical infrastructure entities, works closely with the ASD in co-operation with its Critical Infrastructure Uplift Program (CI-UP) which regularly provides advice and recommendations to further secure Powerlink's assets through targeted investments.

Driver 3: Managing the Evolving Cyber Security Threat

While the ISMP provides overarching governance and maturity maintenance, Powerlink also undertakes a targeted program of cyber security uplift investments to address specific technical cyber security issues. Given the rapidly changing cyber security threat environment, the scope and plan for these Cyber Security Strategic Uplift investments is emergent on an ongoing basis.

Investments under this driver tend to be:

- The implementation of technical solutions to directly address an emergent cyber security threat.
- The implementation of tooling and/or processes to increase Powerlink's threat intelligence and/or incident response capabilities against an emerging trend of threats.

2.3 Compliance Requirements

Relevant cyber security compliance requirements for Powerlink operating as an Australian TNSP within the state of Queensland include the following.

- **Federal Legislation (SOCI/SLACIP)**

  As described in Section 2.2 Driver 2 (page 13) Powerlink is subject to the Security of Critical Infrastructure Act 2018 (SOCI Act) and its 2022 amendment via the Security Legislation Amendment (Critical Infrastructure Protection) Act (SLACIP). Under these laws, Powerlink must establish and maintain a Critical Infrastructure Risk Management Program (CIRMP) that addresses cyber and other security risks.

  The legislation imposes binding obligations for cyber risk management. This includes that Powerlink must adopt a recognised cyber security framework and demonstrate ongoing compliance. Powerlink has chosen the AESCSF to fulfill this requirement, as it is sector-specific and endorsed by regulators (AEMO and the Australian Cyber Security Centre). There is no explicitly mandated maturity level in the Act. Instead, each entity sets its target based on risk.

  Compliance therefore entails keeping our AESCSF-aligned controls effective and up-to-date. Additionally, SOCI rules allow government to introduce mandatory cyber maturity standards in future if deemed necessary. It is anticipated that in the next few years regulators may set higher baseline requirements (for example, requiring [redacted] explicitly for TNSPs).

- **State Policy (Queensland IS18) and the Queensland Government Owned Corporations Act**

  As a Government-Owned Corporation (GOC), Powerlink aligns its security practices with the Queensland Government Information Security Policy (IS18:2018). IS18 requires agencies (and by extension, strongly encourages GOCs) to manage information security in line with ISO 27001 principles and report on maturity.

  While Powerlink's primary benchmark is AESCSF, there is substantial overlap. By meeting AESCSF requirements, Powerlink inherently satisfies most IS18 controls (e.g. having an ISMS, conducting regular assurance, user training etc.). The strategy to use Microsoft's government-aligned security blueprints (which incorporate Australian Signals Directorate ISM controls [redacted] Essential Eight Maturity [redacted] ensures Powerlink's technical controls will eventually meet or exceed Queensland Government standards for confidentiality and resilience.

- **Australian Privacy Act 1988 and subsequent amendments**

  Under the Privacy Act, Powerlink has an obligation to protect personal information collected, stored and managed by the organisation. Powerlink must also comply with the Australian Privacy Principles (APPs) regarding the collection, use, disclosure and security of personal information.

- **Queensland Public Records Act 2023**

  Under the Public Record Act in Queensland, Powerlink has obligations for the management, retention and disposal of records, including requirements to maintain accurate and complete records of activities, decisions and transactions for transparency and accountability. Additionally, Powerlink is required to protect the integrity and security of these records, ensuring they are accessible and preserved for future reference.

- **Risk Management and Corporate Governance**

  The Powerlink enterprise risk management framework drives the need for this investment. Cyber security risk is identified on the corporate risk register, with a target level set by the Board. Powerlink's Board has defined

a risk appetite that no significant cyber risks be rated higher than [redacted] after treatment. Under a base case (no material new investment), the 2025 Threat Risk Analysis (TRA) indicates multiple risks would exceed that threshold by 2032 ([redacted] Such a misalignment with risk appetite would be unacceptable. Therefore, to meet organisational risk expectations, the program must implement treatments to reduce those risks to acceptable levels.

2.4 Inherent risks

Table 1 below summarises the inherent Powerlink cyber security risks, together with a summary of current mitigations and the escalation outlook for the coming regulatory period.

Key Risks	Current Mitigations	Outlook & Escalation
[redacted]		

Key Risks	Current Mitigations	Outlook & Escalation
[redacted]		

Key Risks	Current Mitigations	Outlook & Escalation
[redacted]		

Key Risks	Current Mitigations	Outlook & Escalation
[redacted]		

Table 1: Inherent Risks

3. Options Analysis

3.1 Investment Options Introduction

This business case explores and analyses the following options to address the investment drivers.

Options	Description
Option 1: Recommended Option "Prudent and Proactive Cyber Security Management"	In this recommended option, Powerlink will invest to: ▪ sustain the organisation's cyber security defence maturity; ▪ address obligations under the SOCI Act and ASD guidance; and to ▪ progressively manage the evolving cyber security threat.
Option 2: Alternative Option "Cyber Security Defence Uplift and Risk Minimisation"	In this alternative option, Powerlink will invest to: ▪ **Uplift security practices to AESCSF [redacted] maturity; and** ▪ **Grow internal forward-facing teams with a focus on minimising cyber security risk to wherever feasible.**
Base Case: Counterfactual	In this base case scenario, Powerlink would **not** invest in cyber security controls or further threat mitigation for the medium term.

Table 2: Business Case Options

3.2 Option 1: Recommended Option (Prudent and Proactive Cyber Security Management)

This Recommended Option (Prudent and Proactive Cyber Security Management) describes the planned investment included within the coming regulatory control period proposal. In this option, Powerlink will invest in cyber security management and controls to address the investment drivers identified in section 2.1 and the inherent risks described in section 2.4 as described below.

3.2.1 Recommended Option – Scope Description

Initiative 1: Sustaining Cyber Security Defence Maturity

Threat and risk, external assessments and cyber incidence response test events

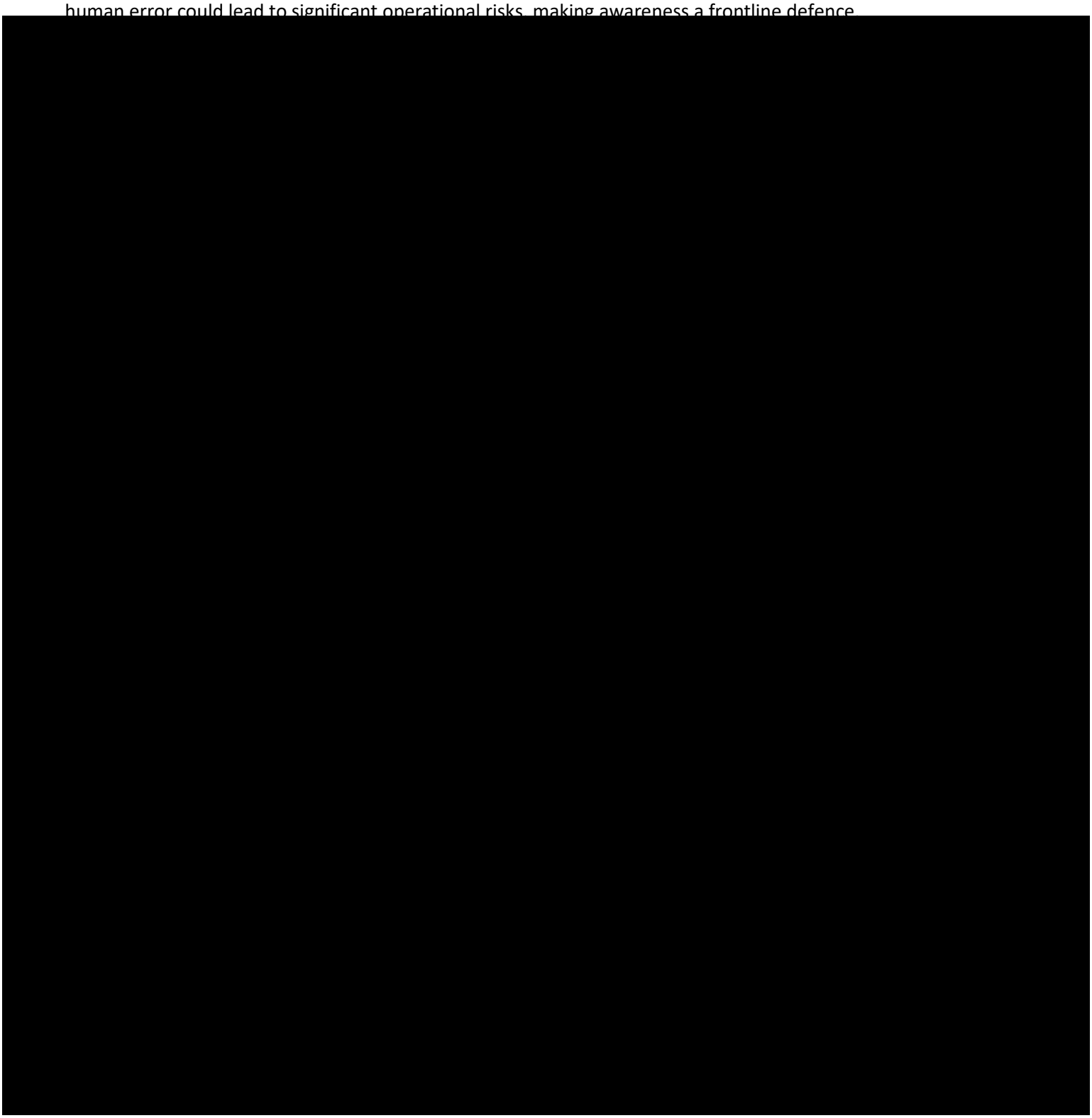
Regular external assessments to validate the effectiveness of internal controls and identify emerging threats before they impact operations. Cyber incident response tests will ensure that teams can react swiftly and minimise downtime in the event of a breach, which is critical for maintaining power network reliability. These exercises also strengthen collaboration between IT and OT environments, reducing the risk of cascading failures across the organisation.

Enhancement of incident playbooks and Business Continuity Plan (BCP) responses

Playbooks will be updated to ensure that response actions remain aligned with evolving threat landscapes and regulatory requirements. Enhanced BCP responses safeguard critical business operations during cyber or physical disruptions, minimising service interruptions. This proactive approach also builds resilience against supply chain vulnerabilities and extreme weather events impacting infrastructure.

Cyber security awareness training programs

Training programs will be delivered to continuously empower employees to recognise and respond to phishing, social engineering, and other common attack vectors. Given the nature of Powerlink's operations, the possibility of human error could lead to significant operational risks, making awareness a frontline defence



[redacted]

Initiative 2: SOCI Act and Proactive Risk Mitigation

[redacted]

[redacted]

Initiative 3: Managing the Evolving Cyber Security Threat

[redacted]

[redacted]

3.2.2 Recommended Option – Assumptions

Table 3 to Table 5 (below) summarise the forecast cost breakdown for each of the three (3) constituent cyber security initiatives. Table 6 (over page) summarises the total combined cost forecast.

Initiative 1: Sustaining Cyber Security Defence Maturity					
FY27 Real Terms	**IT Capex**	**IT Project Opex**	**OT Capex**	**Sec. Systems Field Engineering Capex**	**Total**
Labour	[redacted]				
Vendors					
Software					
Infrastructure					
Total	**$4.0M**	**$14.8M**	**$19.0M**	**-**	**$37.9M**

Table 3: Cost Breakdown – Initiative 1 Sustaining Cyber Security Defence Maturity

Initiative 2: SOCI Act and Proactive Risk Mitigation					
FY27 Real Terms	**IT Capex**	**IT Project Opex**	**OT Capex**	**Sec. Systems Field Engineering Capex**	**Total**
Labour	-	[redacted]			
Vendors	-				
Software	-				
Infrastructure	-				
Total	**-**	**$12.4M**	**$5.5M**	**$20.5M**	**$38.4M**

Table 4: Cost Breakdown – Initiative 2 SOCI Act and Proactive Risk Mitigation

Initiative 3: Managing the Evolving Cyber Security Threat					
FY27 Real Terms	**IT Capex**	**IT Project Opex**	**OT Capex**	**Sec. Systems Field Engineering Capex**	**Total**
Labour	[redacted]				
Vendors					
Software					
Infrastructure					
Total	**$5.5M**	**$11.2M**	**$3.6M**	**-**	**$20.3M**

Table 5: Cost Breakdown – Initiative 3: Managing the Evolving Cyber Security Threat

Total Cyber Program					
FY27 Real Terms	IT Capex	IT Project Opex	OT Capex	Sec. Systems Field Engineering Capex	Total
Labour	[redacted]				
Vendors					
Software					
Infrastructure					
Total	**$9.6M**	**$38.4M**	**$28.1M**	**$20.5M**	**$96.6M**

Table 6: Cost Breakdown - Overall Cyber Program

3.2.3 Recommended Option – Benefits

This recommended option enables benefits as summarised in Table 7 below.

Benefit Description	Benefit Value
B1. Protection of critical infrastructure Effective cyber security controls safeguard the Powerlink electricity transmission network from cyber-attacks that could disrupt power delivery. A strong security posture ensures operational continuity and prevents cascading failures of operational electricity network services grid.	**Non-Financial** **Risk Mitigation**
B2. Operational resilience and business continuity Strong cyber security measures strengthen resilience against incidents that could impact transmission network operations. Rapid detection and response capabilities minimise service interruptions and financial losses during cyber events. Avoidance or minimisation of electricity service interruptions similarly avoids societal costs and impacts across the community.	**Non-Financial** **Resilience and Risk Mitigation**
B3. Ongoing compliance Effective cyber security management enables Powerlink to meet its compliance obligations, including as detailed in Sections 2.2 and 2.3.	**Non-Financial** **Compliance**
B4. Stakeholder confidence and trust Strong cyber security practices build confidence among customers, regulators and partners. Demonstrating robust security controls builds and maintains trust with stakeholders that critical infrastructure is protected against evolving threats.	**Non-Financial** **Stakeholder and Community**

Table 7: Recommended Option (Prudent and Proactive Cyber Security Management) Benefits

3.2.4 Recommended Option – Risk Mitigation

This recommended option mitigates the existing inherent risks (as described in Table 1 on page 15) as summarised below.

Key Risks	Risk mitigation through this option
[redacted]	

Key Risks	Risk mitigation through this option
[redacted]	

Key Risks	Risk mitigation through this option
[redacted]	

Table 8: Recommended Option (Prudent and Proactive Cyber Security Management) Risk Mitigation

3.3 Option 2: Alternative Option (Cyber Security Defence Uplift and Risk Minimisation)

This Alternative Option (Cyber Security Defence Uplift and Risk Minimisation) describes an alternative pathway to address the investment drivers identified in section 2.1 and the inherent risks identified in section 2.4 as summarised below.

3.3.1 Alternative Option – Scope Description

In this option, all measures will be taken to uplift Powerlink's cyber security defences, in order to minimise all viable risk. For planning purposes, this represents a defence uplift to a [redacted], along with ongoing maintenance and operation of those defences.

The scope of this option is therefore additive to the recommended option (i.e. Option 1), with additional scope considerations as summarised below.

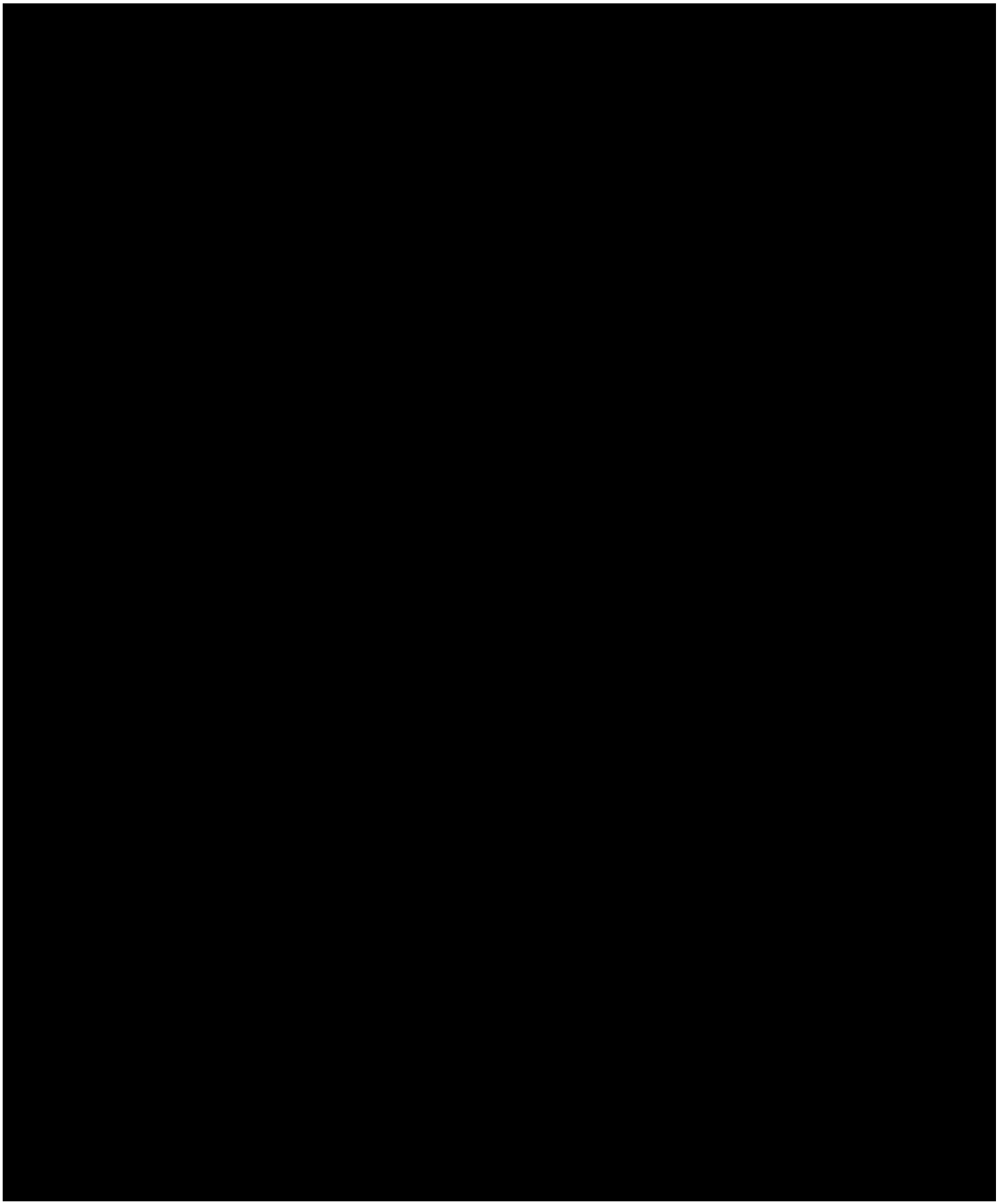
OT Network

[redacted]

Physical and Logical Separation of IT and OT

As a principle, isolation and segregation of IT from OT, requires that OT systems should not be hosted within the IT network.

Where possible all OT systems directly related to control and operation of the network should remain on-premise.



[redacted]

[redacted]

3.3.2 Alternative Option – Assumptions

As noted in section 3.3.1, the scope of Option 2 is additive to the recommended option (i.e. Option 1).

The forecast cost range for the additional scope is estimated to fall in the range of $50-$60M (over five years) in addition to the costs forecast for Option 1.

3.3.3 Alternative Option – Benefits

This recommended option enables benefits as summarised in Table 9 below.

Benefit Description	Benefit Value
B1. Protection of critical infrastructure Maximum cyber security controls safeguard the Powerlink electricity transmission network from cyber-attacks that could disrupt power delivery. The very strong security posture ensures operational continuity and minimises the chance of cascading failures of operational electricity network services grid.	**Non-Financial** **Risk Mitigation**
B2. Operational resilience and business continuity Maximising Powerlink's cyber security defences strengthen resilience against incidents that could impact transmission network operations. Rapid detection and response capabilities minimise service interruptions and financial losses during cyber events. Avoidance or minimisation of electricity service interruptions similarly avoids societal costs and impacts across the community.	**Non-Financial** **Resilience and Risk Mitigation**
B3. Ongoing compliance As per the recommended option (Option 1), effective cyber security management enables Powerlink to meet its compliance obligations, including as detailed in Sections 2.2 and 2.3.	**Non-Financial** **Compliance**
B4. Stakeholder confidence and trust Strong cyber security practices build confidence among customers, regulators and partners. Demonstrating robust security controls builds and maintains trust with stakeholders that critical infrastructure is protected against evolving threats. In this Option 2, a decision to maximise Powerlink's cyber security defences may further improve stakeholder confidence, however this perception would be weighed against considerations of the prudence of increased cost.	**Non-Financial** **Stakeholder and Community**

Table 9: Alternative Option (Cyber Security Defence Uplift and Risk Minimisation) Benefits

3.3.4 Alternative Option – Risk Mitigation

This alternative option mitigates the existing inherent risks (as described in Table 1 on page 15) as summarised below.

Table 10: Alternative Option (Cyber Security Defence Uplift and Risk Minimisation) Risk Mitigation

3.4 Base Case: Counterfactual

The Base Case summarises the counterfactual scenario that would eventuate if Powerlink does not proceed with investment in either the Recommended Option or the Alternative Option to address the investment drivers identified in section 2.1 and the inherent risks identified in section 2.4.

Powerlink considers it unacceptable and infeasible to operate without continued cyber security vigilance and threat response. Therefore, the base case is described here as an “unviable” alternative.

3.4.1 Base Case – Assumptions and Risk Mitigation

As no material actions are taken in the base case to mitigate the existing inherent risks (as described in in section 2.4), the risk outlook is unchanged in the short term. As the threat and risk environment and technology landscape evolves, the efficacy of the control landscape would rapidly degrade over the regulatory period, increasing risk.

3.5 Option Comparison

Table 11 below compares the extent to which the options (including the base case) address the identified investment drivers. As depicted in the table, Option 1 addresses all of the identified investment drivers and is the recommended option.

Alignment with Investment Drivers			
Investment driver	**Option 1: Recommended Option** (Prudent and Proactive Cyber Security Management)	**Option 2: Alternative Option** (Cyber Security Defence Uplift and Risk Minimisation)	**Base Case** (Counterfactual)
Sustaining Cyber Security Defence Maturity	✓	✓	✗
SOCI Act and Proactive Risk Mitigation	✓	✓	✗
Managing the Evolving Cyber Security Threat	✓	✓	✗

Table 11: Options Comparison

Comparison conclusion

Option 1 "Prudent and Proactive Cyber Security Management" is recommended on the basis that it addresses all the identified business and technical investment drivers.

Option 2 "Cyber Security Defence Uplift and Risk Minimisation" is also a suitable response to the investment drivers, but the higher cost of this alternative option likely outweighs the possible incremental future benefits that may be enabled.

4. Cyber Security Governance, Roles and Responsibilities

Effective governance is a critical element of Powerlink's cyber security management. The organisation has established clear roles, responsibilities and oversight mechanisms to ensure that security controls are implemented consistently and that cyber risks are managed appropriately at all levels.

Key aspects of the governance structure are summarised in the following sections.

4.1 Executive Oversight and Governance Committees

Powerlink's cyber security initiatives are overseen by a senior executive committee known as the Information Security Senior Governance Group (ISSGG).

The ISSGG comprises senior stakeholders, including executives from IT, OT (network operations), Risk/Compliance, and other business units. This group meets regularly to review the status of the cyber security program and related projects, assess emerging risks, and make strategic decisions (such as approving major investments or policy changes).

The ISSGG provides program governance by monitoring all security initiatives and ensuring they align with corporate objectives. If a large security project is managed separately (for example, a major OT security retrofit), it still reports into this governance group for visibility and coordination. This top-down governance ensures cyber security has visibility at the highest levels and that cross-department support is in place.

In addition to the ISSGG, cyber security performance and issues are reported to the Executive Leadership Team and the Board (or a Board Risk/Audit Committee) periodically. This includes metrics like compliance status, incident summaries, and maturity assessments. High-level oversight by the Board underscores cyber security as a critical governance issue in line with fiduciary duties and regulatory expectations.

4.2 Cyber Security Leadership and Functions

Responsibility for cyber security lies with specialised roles and teams. Powerlink has a Cyber Security Manager (equivalent to a CISO role) responsible for leadership of the cyber security delivery program, and is the primary authority on cyber matters. This leader is responsible for executing the strategy, managing security staff, and reporting status and risks to executives/ISSGG.

Key functions:

- **IT Security** manages security of enterprise IT systems (network security, endpoint protection, identity management, cloud security configuration, etc.).
- **OT Security** focuses on securing operational technology (substation systems, SCADA networks).
- The **Security Operations Centre (SOC)** function monitors logs and alerts from across IT and OT in real time, looking for signs of intrusion or anomalies, and coordinates incident response. The SOC follows defined playbooks, with established escalation paths when a threat is detected.
- **Risk and Compliance Management** ensures security policies and controls meet regulatory requirements (SOCI Act, privacy laws, etc.), manages cyber risk assessments, and handles audits.

- **Project Management and Security Architecture,** working within the cyber security delivery program to plan and implement specific uplift projects (for instance, rolling out a [redacted]

4.3 Other Key Roles and Responsibilities

Powerlink's governance framework delineates responsibility for implementing and maintaining controls, with the following key roles and responsibilities.

- **System/Asset Owner Roles:** These roles are designated for critical systems or datasets, with accountability for ensuring proper security controls on those assets in alignment with policies. For example, the owner of the Advanced Energy Management System (AEMS) must ensure that patches are applied and only authorised personnel are granted access.
- **Incident Response Team Roles:** Powerlink has an Incident Response Plan that defines specific roles including Incident Coordinator, Communications Lead, Forensic Analyst, etc. When a serious incident occurs, these roles are activated, often drawing personnel from IT, OT, corporate communications and legal services as needed. Everyone knows their role in advance (through training and drills), which streamlines response in a crisis.
- **Integration of IT and OT Governance:** Recognising convergence between IT and OT systems, Powerlink integrates governance across these domains. Rather than siloed decision-making, the governance structure (ISSGG and security leadership) spans both IT and OT. For example, the ISSGG reviews both IT security metrics (e.g. phishing test success rates) and OT security metrics (e.g. number of substations with monitoring in place). The cyber security program governance includes operations managers when assessing OT risks and planning mitigations, ensuring that security measures do not inadvertently disrupt power system reliability. This integrated approach ensures consistent risk management while respecting domain differences.
- **Regulatory and Audit Governance:** The SOCI Act requires executive attestation of the risk management program, which must be built into governance routines (the ISSGG or Board receives updates on the CIRMP controls). Powerlink undergoes annual AESCSF assessments and participates in sector-wide benchmarking coordinated by AEMO, with the results reviewed at the executive level and action plans formulated for any weakness. Similarly, internal audits (and periodic external audits, including those undertaken by the Queensland Audit Office) review cyber security effectiveness. Governance teams track any audit findings to closure. There is also coordination with government (e.g. liaison with the Australian Cyber Security Centre for threat intelligence and with regulators for incident reporting), ensuring that Powerlink's governance not only looks inward but also engages with external oversight bodies.
- **All Employees and Contractors** have responsibilities outlined in the Acceptable Use Policy and other policies. They must follow security procedures (like not sharing passwords, reporting phishing attempts), complete regular security awareness training, and report any security incidents or suspicious activity promptly. Accountability for following these rules is enforced through Human Resources processes.
- **Third-Party Partners/Vendors** have security responsibilities enforced via contracts and onboarding processes. Vendors with network access must comply with Powerlink's security requirements (e.g. use MFA, have up-to-date antivirus on their systems). Contracts often include clauses for security (right to audit,

incident notification). Internally, vendor management roles oversee that vendors meet these obligations, and critical suppliers might be required to provide regular security attestations.

Overall, Powerlink's governance model establishes clear accountability from the Board level down to individual system custodians. With formal governance committees, responsible security leadership, and defined roles at every level, Powerlink embeds cyber security into corporate governance. This structure enables informed decision-making balancing security investments with other business needs, and ensures that when urgent action is needed, the decision pathways are clear and authority is established. Strong governance also fosters a culture of security, where it's viewed as everyone's responsibility and gets the necessary attention and resources from senior management.

5. Cyber Security Policies

Powerlink has developed a comprehensive set of information security policies to guide the organisation in protecting its assets and managing cyber security risk. These policies align with industry standards and regulatory requirements, and they are periodically reviewed and updated to remain effective amid changing threats.

Key policies and policy areas include:

- **Information Security Policy:** This top-level policy establishes Powerlink's commitment to information security and sets high-level objectives. It outlines the scope (including all information assets, IT and OT systems, and personnel) and defines the overall governance structure. It mandates compliance with AESCSF practices and other relevant standards, and is endorsed by senior management, signalling that security is a priority across the organisation.
- **Access Control Policy:** Governs how access to systems and data is managed. It enforces "least privilege" principles, whereby users and administrators are granted only the minimum access needed for their roles. This policy covers user account management (creating accounts, periodic access reviews, and timely removal of access when staff leave or change roles), password standards (length, complexity, and rotation requirements), and multi-factor authentication for sensitive systems. It also includes management of privileged accounts through a Privileged Access Management (PAM) system, ensuring administrative access is tightly controlled (with measures like just-in-time access and session recording planned as future enhancements). For OT systems, it specifies additional rules for remote access (e.g. use of jump-hosts and one-time approval for any vendor access). By adhering to this policy, Powerlink reduces the chance of unauthorised access or credential misuse.
- **Acceptable Use Policy (AUP):** Informs employees and contractors of their responsibilities when using company IT resources. It details what is considered acceptable (e.g. using corporate devices for business purposes, minimal personal use) and prohibited activities (such as installing unauthorised software, connecting unapproved devices to the network, or using corporate email for personal sensitive communications). It also addresses safe use of email and internet (caution against clicking unknown links, etc.), social media guidelines as a representative of the company, and the handling of confidential information (e.g. not transferring it to personal accounts or cloud services). The AUP helps reduce risky behaviour that could lead to malware infections or data leakage by setting clear expectations.
- **Data Handling, Retention and Disposal Policies:** Powerlink maintains policies on information classification and handling. An Information Classification Policy defines data categories (e.g. Public, Internal, Confidential, Highly Sensitive) and describes required protections for each (such as encryption for highly sensitive data at rest and in transit, or marking documents as "Confidential"). A Media Handling Policy covers secure use of removable media (USB drives must be encrypted and usage is monitored) and proper disposal of media (shredding or secure wiping of drives). A Data Retention and Disposal Policy ensures data is retained for required periods and then disposed of securely. These policies ensure that information is identified and safeguarded according to its sensitivity throughout its lifecycle.
- **Cyber Incident Response Policy:** Describes the process to follow in the event of a security incident. It defines what constitutes an incident and sets the framework for incident handling (following the prepare, detect, respond, recover phases). It establishes an Incident Response Team and clarifies each team member's role

(incident lead, communications lead, etc.). The policy requires that all incidents be logged and investigated, and that serious incidents be escalated promptly (and to external authorities as required by law, such as the Australian Cyber Security Centre under SOCI reporting rules). It references detailed incident response playbooks for specific scenarios (like ransomware, loss of a laptop with data, DDoS attack, etc.). This policy ensures a consistent and effective response to minimise damage when incidents occur.

- **Change Management and Secure Development Policies:** Powerlink has a Change Management Policy to integrate security into IT system changes. It requires that any significant change (new system, major update) undergo a security risk assessment and, where appropriate, a penetration test before going live. This prevents inadvertently introducing vulnerabilities. A Secure Software Development Policy (or secure coding standards) is in place to guide any in-house software developers or those customising vendor software, covering topics including input validation, authentication and regular code review for vulnerabilities. These policies aim to ensure that new systems or features are built securely from the start (aligning with the principle of "security by design").

- **OT-Specific Cyber Security Policy:** Because OT (industrial control) systems have unique constraints, Powerlink includes guidance specific to OT. This addresses areas including patch management in OT (acknowledging that patches must be carefully scheduled and tested to avoid disrupting operations), baseline secure configurations for OT devices (disabling unused services, default passwords changed), and physical security requirements for critical OT sites. It codifies network segmentation principles such as "IT and OT networks shall only connect via defined intermediaries (firewalls, data diodes) and sensitive OT sub-networks shall be isolated." It also addresses other OT-specific incident response practices. By having OT-specific rules, Powerlink ensures the policies are practical and effective for the operational environment.

- **Vendor and Third-Party Security Policy:** Given the supply chain risks, Powerlink has policies governing third-party access and procurement. This policy requires security vetting of vendors, including that critical vendors might need to have certain certifications (like ISO 27001) or complete a security questionnaire. Contracts with suppliers of IT or OT systems must include security and continuity clauses (e.g. the supplier will support timely patching of their product, will notify Powerlink of any breaches in their organisation, and will provide an SBOM for software). The policy also dictates that any third-party connecting to Powerlink's network must agree to Powerlink's security terms (e.g. use of MFA, not connecting from unknown devices, etc.). Additionally, it sets expectations for cloud providers and SaaS, requiring data residency considerations and clarity on shared security responsibilities. With this, Powerlink extends its security governance into its supply chain.

- **Compliance and Audit Policy:** To ensure these policies are followed, Powerlink has processes for compliance attestation and audit. Employees may be required to sign an acknowledgment of key policies annually. The internal audit plan often includes reviewing adherence to security policies (for example, an audit might check if accounts of departed employees were disabled in the timeframe specified by policy). Deviations from policy (exceptions) must be approved and documented (e.g. if an OT system cannot technically meet a requirement, a compensating control and formal exception are recorded). This ensures that exceptions are known, managed and revisited to see if they can be closed later.

Powerlink's cyber security policies are living documents. They are reviewed on a regular cycle (typically annually or whenever significant changes occur in the business or threat landscape). For example, if a new type of threat

emerges or if regulators issue new guidelines, the relevant policy is updated.

Within the remit of the Powerlink Cyber Security Program is to update documentation and embed new processes. When new security measures are implemented (e.g. a new privileged access management tool or an AI monitoring system), policies and procedures are revised to reflect how to use and maintain these controls. This ensures policies remain up-to-date and actionable rather than static paperwork.

Crucially, these policies are communicated and accessible to all employees. Through security awareness programs and training, staff learn the key points of policies so they understand their responsibilities.

Compliance is also enforced. For example, failing phishing tests or not completing mandated training might result in remedial training or escalation to managers. Repeated or wilful violations of security policies can lead to disciplinary action, underscoring that cyber security is taken seriously.

Powerlink's suite of cyber security policies provides a clear and structured approach to managing controls, ensuring consistency, accountability and compliance. They form the foundation on which technical measures and procedures are built, and they evolve alongside the threat landscape and Powerlink's business needs.

6. Glossary of Terms

Term	Definition
aaS	as-a-Service
AEMO	Australian Energy Market Operator
AEMS	Advanced Energy Management System
AI	Artificial Intelligence
ACSC	Australian Cyber Security Centre
AESCSF	Australian Energy Sector Cyber Security Framework
APP	Australian Privacy Principles
ASD	Australian Signal Directorate
AUP	Acceptable Use Policy
BCP	Business Continuity Plan
CASB	Cloud Access Security Broker
CI	Critical Infrastructure
CIRMP	Critical Infrastructure Risk Management Program
CISO	Chief Information Security Officer
CI-UP	Critical Infrastructure Uplift Program
CSIWG	Cyber Security Industry Working Group
DDoS	Distributed Denial-of-Service
DSPM	Data Security Posture Management
DLP	Data loss prevention
E-CAT	Electricity Criticality Assessment Tool
ECC	Elliptic Curve Cryptography
ECSO	Enhanced Cyber Security Obligations
EDR	Endpoint Detection and Response
ERP	Enhanced Response and Prevention
GOC	Government-Owned Corporation
IDAM	Identity and Access Management
IEC	International Electrotechnical Commission
ISMP	Information Security Management Program
ISMS	Information Security Management System
ISO	International Organisation of Standardisation

Term	Definition
ISSGG	Information Security Senior Governance Group
IT	Information Technology
MFA	Multi Factor Authentication
NIST	National Institute of Standards and Technology
NPV	Net Present Value
OT	Operational Technology
PAM	Privilege Access Management
RSA	Rivest-Shamir-Adleman
SBOM	Software Bills of Materials
SCADA	Supervisory Control and Data Acquisition
SLACIP	Security Legislation Amendment Critical Infrastructure Protection
SOC	Security Operations Centre
SOCI	Security of Critical Infrastructure Act
SOE	Standard Operating Environment
SoNS	Systems of National Significance
TRA	Threat Risk Assessment
TNSP	Transmission Network Service Provider
USB	Universal Serial Bus
VPN	Virtual Private Network
XDR	Extended Detection and Response