AusNet

Transmission Revenue Reset

TRR (2027-32)

Cyber Security Business Case

Friday, 31 October 2025

Table of contents

Document history

DATE	VERSION	COMMENT
16/08/2025	V1.0	Initial draft business case for review
11/09/2025	V2.0	Revised business case incorporating input
06/10/2025	V3.0	Updated for final review
28/10/2025	V4.0	Final business case document

Related documents

DOCUMENT	VERSION	AUTHOR
Technology Strategy and Investment Plan	V2.0	AusNet Services
Digital Program NPV Model	V2.0	AusNet Services

Approvals

POSITION	DATE
Digital & Technology – Strategy, Regulatory and Partner Management	October 2025
Digital & Technology – Cyber Security	October 2025
Digital & Technology – Architecture	October 2025

Executive summary

AusNet operates more than 200 digital applications and systems supported by a mix of on-premises and cloud-hosted infrastructure. In the next regulatory period, we will further expand our digital services to enhance our network operations, asset management, customer and landholder experience, and productivity.

The rapid integration of distributed energy resources, advanced metering, automation, and real-time data exchange is transforming the energy ecosystem into a more dynamic, interconnected, and interdependent environment. While this digital transformation is essential to enable a low-carbon and efficient future, it also broadens the cyber-attack surface and exposes critical infrastructure to increasingly sophisticated and persistent threats.

As our reliance on technology grows, so does the need to ensure that our digital assets and systems remain resilient against cyber threats and operational disruptions. A successful cyber-attack on electricity networks such as AusNet could have severe consequences, including:

- Disruption to electricity services
- Impacts on public safety
- Compromise of data privacy
- Loss of control over critical digital systems

The expansion of our digital footprint is occurring in parallel with a heightened and increasingly complex cyber threat landscape. Threat actors are intensifying their activities, demonstrating increasing determination, sophistication, and persistence. Australia and critical infrastructure continue to face a rapidly evolving cyber threat environment, driven by heightened geopolitical tensions, strategic competition in the Indo-Pacific, and the growing interconnectivity of critical infrastructure systems. In 2024, the Five Eyes intelligence alliance, including the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), publicly attributed the (C-I-C), to the compromise of multiple United States critical infrastructure networks, intended to pre-position for potential disruptive or destructive attacks. Similar activity has been linked to (C-I-C), (C-I-C) targeting critical infrastructure across the United States, Australia, and other Five Eyes nations. In parallel, (C-I-C) groups have continued to target global energy and infrastructure systems, underscoring the transnational and persistent nature of the threat landscape.

(C-I-C)

In October 2025, the Australian Signals Directorate (ASD) released its Annual Cyber Threat Report 2024–2025, highlighting a rapidly intensifying cyber threat landscape, particularly across Australia's critical infrastructure sectors. A new cyber incident is now reported every six minutes, with ASD responding to more than 1,200 incidents in the past year. The report emphasised a marked escalation in state-sponsored activity, with nation-state (C-I-C), continuing to target Australian organisations. These actors are well-resourced, highly coordinated, and remain focused on espionage and pre-positioning within networks to enable future disruptive or destructive operations. ASD further observed a 111% increase in outbound referrals of potentially malicious activity targeting critical infrastructure organisations, signalling the growing strategic focus of hostile actors on sectors essential to Australia's economic resilience and national security.

In addition to state-sponsored threats, the rise of ransomware-as-a-service, AI-enabled attack campaigns, and vulnerabilities in third-party software have lowered the barriers to entry for malicious actors, amplifying risks to organisations such as AusNet. The convergence of Information Technology (IT) and Operational Technology (OT) environments further compounds this risk by increasing the number of potential entry points and the depth of system compromise available to attackers.

A recent Tech Business News survey found that 79% of Australian IT leaders believe that geopolitical tensions are exacerbating the cyber threat landscape, reinforcing the imperative for sustained investment in cyber resilience to protect the reliability and security of the national energy system.

These developments reinforce the need for sustained investment in cybersecurity.

As a Transmission Network Service Provider (TNSP) operating critical electricity infrastructure essential to the Victoria and Australia, AusNet represents a potential target for nation-state and criminal actors seeking to disrupt essential services, compromise operational technology (OT) environments, or exploit supply chain interdependencies.

Digital transformation of our business, which is critical for the ongoing efficient management of our network and provision of services to our customers, has potential to expand the attack surface of our business and therefore

increase our risks. As more digital systems connect to our network, there is more convergence and interconnection between IT and OT and therefore more pathways for a cyber attack to spread across all systems and impact our services. This is compounded by our interconnection with Distribution Network Service Providers (DNSP), both through the network and network control systems (Operational Technology), which creates an additional area of risk at the interface between businesses.

In response to the escalating cyber threat landscape, the increasing digitalisation of energy systems, and the developments in the sector's cyber security framework requirements, AusNet has developed a comprehensive, risk-based Cyber Resilience Strategy and roadmap. This strategy is designed to strengthen and uplift cybersecurity capabilities, thereby enhancing the resilience, reliability, and safety of AusNet's operations. The Cyber Resilience Strategy comprises:

- Recurrent expenditure, to maintain, update, and optimise existing cybersecurity systems and technologies, ensuring continued functionality, compliance, and resilience.
- Non-recurrent expenditure, to implement new systems, tools, and practices that mitigate emerging threats and uplift performance in line with recognised industry frameworks.

AusNet takes a risk-based approach to managing cyber threats and risks, adopting best industry practice, to achieve reduction of risks as far as reasonably practicable. This approach aligns with the criticality of our operations and the expectations of our stakeholders to protect our digital assets, energy networks, and our customers. Maintaining the current level of cyber maturity is not a credible or sustainable option, as the effectiveness of controls will deteriorate over time, increasing exposure to unacceptable risk to the organisation and its stakeholders.

To maintain alignment with regulatory obligations under the Security of Critical Infrastructure (SOCI) Act and consistency with the Australian Energy Sector Cyber Security Framework (AESCSF), AusNet has adopted Version 2 (V2) of the AESCSF. Developed collaboratively by AEMO, government, and industry, AESCSF V2 aligns with international standards and addresses emerging technologies and threats. While the framework does not prescribe specific Security Profiles (SPs), AEMO recommends that participants target higher levels of maturity commensurate with their criticality and risk exposure.

We assessed the need for investment to maintain the existing systems and practices (recurrent expenditure) as well as investment in new systems and practices (non-recurrent expenditure) to manage cyber security maturity levels:

- Recurrent expenditure Option 1: actively manage without vendor support (counterfactual option)
- Recurrent expenditure Option 2: perform lifecycle refreshes
- Non-recurrent expenditure Option 1: achieve AESCSF Version 2 Security Profile 2 (V2 SP-2)
- Non-recurrent expenditure Option 2: achieve AESCSF Version 2 Security Profile 3 (v2 SP-3)

Recurrent and non-recurrent expenditure are explained separately to simplify the analysis and be clear on the drivers and outcomes. However, these are related and as a result AusNet must select the prudent and efficient combination of the two recurrent and two non-recurrent options. The four possible combinations are set out in Table 1.

Table 1 – Summary of options and assessment outcomes for recurrent expenditure

#	OPTION COMBINATIONS	CAPEX (RECURRENT)	OPEX	RISK ASSESSMENT
1	Recurrent Option 1 only	-	-	Results in increased risk which will cause business-wide disruption
2	Recurrent Option 2 only	$20.41m	-	Degradation of risk position as today's capabilities don't address the evolving cyber threat landscape.
3	Recurrent Option 2 and Non-recurrent Option 1	$47.44m	$14.04m	Improve cyber maturity and reduces the probability of cyber events occurring but does not address the consequence. Does not meet best industry practice or AESCSF recommended maturity level.
4	Recurrent Option 2 and Non recurrent Option 2	$55.06m	$18.0m	Reduces the probability and consequence of cyber events occurring. Achieves best industry practice and AESCSF recommended maturity level.

We recommend proceeding with Option 4. As a high-criticality market participant, AusNet considers it prudent and necessary to operate at an elevated level of cybersecurity maturity. Accordingly, this business case recommends investment to uplift AusNet's cyber capability maturity to achieve Security Profile 3 (SP3) under AESCSF Version 2. Achieving this target state consists of:

- Recurrent expenditure Option 2 to perform lifecycle refreshes to maintain our current cyber security systems and applications, and
- Non-recurrent expenditure Option 2 to enable compliance with 354 practices across our businesses to provide the capability uplift required for AESCSF V2 SP-3

The investment required to achieve this for both recurrent and non-recurrent expenditure is set out in **Table 2**.

Table 2 – Annual expenditure required for cyber security ($m, real 2025, transmission network cost allocation)

Cost item	R2028	R2029	R2030	R2031	R2032	Total
Recurrent capex	4.08	4.08	4.08	4.08	4.08	20.41
Non recurrent capex	6.93	6.93	6.93	6.93	6.93	34.65
Recurrent opex Note	3.60	3.60	3.60	3.60	3.60	18.00
Total	**14.61**	**14.61**	**14.61**	**14.61**	**14.61**	**73.06**

Note: this is recurrent opex that is associated with the new systems implemented under non-recurrent capex so is additional to baseline opex

1. Context

1.1. Background

The rapid integration of distributed energy resources, advanced metering, automation, and real-time data exchange is creating a more dynamic, interconnected, and interdependent energy ecosystem. While this transformation is critical to enabling a low-carbon and more efficient future, it also expands the cyber attack surface and exposes critical infrastructure to increasingly sophisticated and persistent threats and risks.

We operate more than 200 digital applications and systems supported by on-premises and cloud-hosted infrastructure. In the next regulatory period, we will further expand our digital services to enhance our network operations, asset management, customer and landholder experience, and productivity. As we increasingly rely on technology to deliver safe and reliable electricity across Victoria, and to run our business efficiently, the consequences of a successful cyber-attack increases, including:

- Disruption to electricity services
- Loss of control over critical digital systems
- Impacts on public safety
- Compromise of data privacy

Cyber attacks can exploit operational technology (OT) systems or information technology (IT) systems using different methods, but can result in impacts to customers in the form of safety hazards, disruption to services and data breaches. We must ensure that our digital assets are resilient to cyber threats and operational disruptions.

In response to constantly evolving threats and developments in industry cyber security framework requirements, AusNet has developed a Cyber Resilience Strategy and roadmap to develop capabilities and practices across our business. The strategy involves continued investment in existing systems and technologies to ensure they remain functional (recurrent expenditure) and investment in new systems and development of practices to mitigate new and emerging threats and to achieve improved performance based on industry frameworks (non-recurrent expenditure).

AusNet takes a risk-based approach to managing cyber threats and risks, adopting best industry practice, to achieve reduction of risks as far as reasonably practicable. This approach aligns with the criticality of our operations and the expectations of our stakeholders to protect our digital assets, energy networks, and our customers. This business case outlines our proposed investments to uplift our cyber capability maturity to meet Security Profile 3 (SP-3) as defined in Version 2 of the Australian Energy Sector Cyber Security Framework (AESCSF).

1.2. Cyber threat landscape

In 2024, FiveEyes intelligence agencies including the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) publicly attributed (C-I-C) had compromised the networks of multiple United States' (US) critical infrastructure entities across the energy, communications, transport, and water and sewerage sectors, to preposition for destructive attacks on operational technology networks in the event of a crisis. [1]

In their Annual Cyber Threat Report 2023–2024,[2] title "State-sponsored cyber threats: Growing risks for Australia's critical infrastructure", The ASD highlights a rapidly evolving cyber threat landscape, aligning with the challenging strategic environment outlined in the 2024 National Defence Strategy[3] and the 2023-2030 Australian Cyber Security Strategy[4].

ASD's ACSC have assessed that Australian critical infrastructure could be vulnerable to similar activity. [5] Earlier this year, a range of intelligence agencies led by the US Cybersecurity & Infrastructure Security Agency publicly attributed similar adverse cyber activities against a number of critical infrastructure sectors in the US, Australia and other Five Eyes

[1] (C-I-C)
[2] https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024
[3] https://www.defence.gov.au/about/strategic-planning/2024-national-defence-strategy-2024-integrated-investment-program
[4] https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy
[5] (C-I-C)

countries to the (C-I-C)[6]. Additional cyber risks to critical infrastructure have also been attributed (C-I-C) targeting US critical infrastructure, and (C-I-C) actors against global critical infrastructure. [7,8]

(C-I-C)

Emerging threats such as ransomware-as-a-service, AI-enabled attacks, and vulnerabilities in third-party software have lowered barriers to entry and increased the risk to AusNet. A survey by Tech Business News found that 79% of Australian IT leaders believe that global geopolitical tensions are only worsening the threat.[9]

Further complicating the cyber threat is the convergence of IT and OT systems which increase the extent and locations that are vulnerable to attack and the extent to which an attack can penetrate the systems. To ensure the security of our systems while operating within this cyber threat landscape, and to address regulatory pressures under frameworks like SOCI and AESCSF, AusNet has developed a comprehensive, risk-based cyber security strategy.[10]

1.2.1. Threats to Operational Technology (OT) systems

The digitalisation of Australia's electricity networks is transforming how Transmission Network Service Providers (TNSPs) and Distribution Network Service Providers (DNSPs) plan, operate, and interact. This transformation is critical to achieving a modern, flexible, and decarbonised energy system but also introduces new cybersecurity, interoperability, and operational risks that must be managed to maintain network reliability and resilience.

Within our transmission network, digitalisation is advancing through Advanced Energy Management Systems (AEMS), Phasor Measurement Units (PMUs), field mobility, and digital substations. These technologies improve operational resilience, system efficiency, stability, and situational awareness but also extend the network's digital footprint and potential attack surface.

Across distribution networks, technologies such as Advanced Metering Infrastructure (AMI), Advanced Distribution Management Systems (ADMS), and Distributed Energy Resource Management Systems (DERMS) are enabling near real-time visibility of consumption, generation, and grid performance. While these systems enhance efficiency and customer engagement, they deepen interconnections between distribution and transmission networks, increasing interdependency and shared exposure to cyber threats. Recent regulatory requirements for DNSPs to monitor and control Distributed and Customer Energy Resources (DER/CER) have accelerated the deployment of new operational technology (OT) platforms, such as low-voltage DERMS, that communicate with externally managed assets over public networks. This represents a fundamental shift from traditionally isolated OT environments and significantly broadens the cyber-attack surface. Although such systems sit within the distribution domain, in integrated networks like AusNet's, their security directly affects the resilience of transmission infrastructure through shared data and control interfaces.

Moreover, this digitalisation is expanding the convergence of IT and OT systems. This, coupled with increased automation and remote connectivity, creates new pathways for threat actors and raises the potential for cyber events to propagate across domains. Compromises in IT environments can cascade into OT systems, affecting the availability and safety of essential services.

AusNet's OT environments face material risks such as disruption to electricity services by nation sponsored threat actors, ransomware-induced outages, espionage by nation-state actors, and insider misconfigurations. Specific threats include phishing attacks on OT personnel, external attacks exploiting legacy protocols, data breaches, malware

[6] [C-I-C]
[7] (C-I-C)
[8] (C-I-C)
[6] (C-I-C)
[9] *Australia Under Attack As Elevated Cyber Threat Activity Observed, Armis Report Finds - Tech Business News*
[10] Cyber Security Strategy and Roadmap, AusNet, May 2025

infiltration, and supply chain vulnerabilities. OT systems are prime targets for malicious cyber threat actors due to several factors, including:

- Their role in supporting the critical infrastructure which underpins the delivery of essential services.
- Their longer operational lifespans (often spanning decades) and slower rate of change compared to Information Technology (IT) systems, often leading to the existence of unpatched security vulnerabilities.
- Their reliance on legacy insecure communications protocols which do not support security controls such as authentication, encryption and non-repudiation.

The increasing digital interconnection between operational technology (OT), information technology (IT), and external ecosystems underscores the urgent need to strengthen OT security. Compromises in IT environments can now cascade into OT systems, jeopardising the availability, reliability, and safety of critical energy operations. Addressing these risks requires enhanced network segmentation, secure remote access, continuous monitoring, and a sustained uplift of cybersecurity capabilities.

While digitalisation is essential to the modernisation of Australia's energy system, it has also expanded the cyber-attack surface. For AusNet, ongoing attention and investment are therefore prudent and efficient to maintain compliance with regulatory obligations, safeguard mission-critical OT systems, and ensure the continued security, reliability, and resilience of energy delivery across the network.

1.2.2. Threats to Information Technology (IT) systems

AusNet's IT systems are exposed to a broad spectrum of cyber threats that can compromise sensitive data and disrupt enterprise operations. Material risks include data breaches, service outages, ransomware attacks, and insider misconfigurations with cascading impacts. These threats encompass social engineering and phishing, external attacks such as DDoS, malware infections, nation-state advanced persistent threats (APTs), third-party vulnerabilities, and internal misuse.

The increasing complexity of AusNet's digital supply chain and dependence on interconnected systems heighten exposure to exploitation. Threat actors actively target critical-infrastructure entities to exfiltrate intellectual property, personal data, and operational intelligence for financial or strategic gain, as well as to cause disruption. To mitigate these risks, AusNet's Cyber Resilience Strategy prioritises initiatives that strengthen protection, detection, and response capabilities such as privileged-access management, secure software-development practices, data-loss prevention, and advanced endpoint protection. These initiatives are designed to reduce risk exposure, ensure compliance with the Australian Energy Sector Cyber Security Framework (AESCSF), and support the continuity and reliability of AusNet's business operations and stakeholder relationships.

1.2.3. Impacts on customers

Cyber threats are malicious activity of unauthorised individuals or organisations that compromise the security of information and communication systems. The threats include attempts to disrupt operations or access data by exploiting weaknesses in digital assets such as infrastructure, applications and systems or devices.

Cyber attacks can lead to severe consequence for electricity networks such as AusNet. A successful attack could compromise control over the physical network and digital systems used to operate the business. In turn, this could cause widespread and prolonged disruption of electricity. As the transmission network service provider for Victoria, the consequences could be severe; potentially leading to prolonged outages for all Victorian electricity customers. The impact to residential customers and economic activity would be extensive. Critically, electricity is also an enabler of other essential services that would have negative consequences for customers:

- **Disruption to Electricity Services:** cyber attacks on OT systems could disrupt the supply of electricity through the transmission system which could affect over 7 million Victorians. AusNet's digital systems are essential to maintaining energy flow across the network, and any compromise—such as ransomware or sabotage—could result in wide spread or state-wide outages. By strengthening OT security, AusNet reduces the risk of service interruptions that could impact homes, businesses, and critical infrastructure such as hospitals and transport systems.
- **Public Safety:** cyber threats to energy infrastructure pose significant risks to public safety. A prolonged disruption in energy services could affect medical supply chains, food distribution, telecommunications, and emergency services. Ensuring system resilience enables continued and undisrupted operation of essential services, thereby safeguarding the wellbeing of the public and minimizing societal disruption.

- **Data Privacy:** AusNet is enhancing its data protection capabilities to address increasing privacy risks and regulatory requirements. These measures help prevent unauthorized access to personal and commercially sensitive data, reducing the risk of identity theft, fraud, and reputational harm for customers.
- **Security of Digital Systems:** As AusNet modernizes its energy network, customers increasingly interact with digital platforms for market data, billing, energy usage insights, and outage notifications. Resilience and security of these systems by embedding cybersecurity into software development, identity management, and endpoint protection is essential to protect customers from digital threats and to enable safe, reliable access to energy-related services and information.

1.3. Regulatory and compliance obligations

Critical infrastructure is a key target of cyber attacks due to the potential for severe consequences. The Australian Cyber Security Centre (ACSC) found recently that about 25 per cent of reported cyber security incidents involved Australia's critical infrastructure, and that electricity sector constitutes 30% of the reported cyber security incidents in critical infrastructure for 2023-2024[11]

Table 3 identifies key regulatory obligations that are critical to AusNet's cyber security practices.

Table 3 - Regulatory obligations underpinning cyber security functions

Regulatory Obligation	Description of obligations
Security of Critical Infrastructure Act 2018 (SOCI Act)	The SOCI Act seeks to manage national security risks in Australia's critical infrastructure including energy. The obligations include: • a requirement to develop a register of Critical Infrastructure Assets • mandatory cyber incident reporting to the Australian Cyber Security Centre • information and directions powers
Privacy Act 1988 and Information Privacy Act 2014	The obligations require us to maintain strong controls and security on the accessibility of customer data as well as appropriate availability of data.
National Electricity Rules	Under section 4.11.2(c) of the NER, we must comply with AEMO's Standard for Power System Data Communications which operates in parallel to the SOCI Act identified above. Section 4 of the Act requires that cyber, physical and network security considerations are appropriately addressed by all parties including through robust programs and reporting frameworks to adequately and continuously manage security risks that could adversely impact power system communications and supporting systems and infrastructure.
Enhanced Response and Prevention Act 2024 (SOCI Amendment Act)	The Act sets out the obligation to manage the cyber risk to the critical infrastructure, including energy sector. The relevant obligations include: • extending critical assets obligation to the systems holding business critical data • responding to the government request to address serious deficiencies within their risk management programs, if any. • Taking direction from the government to manage all hazards incidents
Cyber Security Act 2024	Act seeks a mandatory requirement for reporting of ransomware ransom payments.

[11] https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024

1.4. Industry framework - AESCSF

Consistent with our peers in the sector, AusNet aligns to the Australian Energy Sector Cyber Security Framework (AESCSF) to establish, uplift and measure the maturity of our cyber security capabilities. The AESCSF was developed in 2021 by the Australian Energy Market Operator (AEMO) in collaboration with industry and government stakeholders including the Australian Cyber Security Centre (ACSC), Critical Infrastructure Centre (CIC), and the Cyber Security Industry Working Group (CSIWG) to raise the level of cyber maturity across the energy sector by helping market participants to assess, benchmark, and enhance their cyber security capabilities.

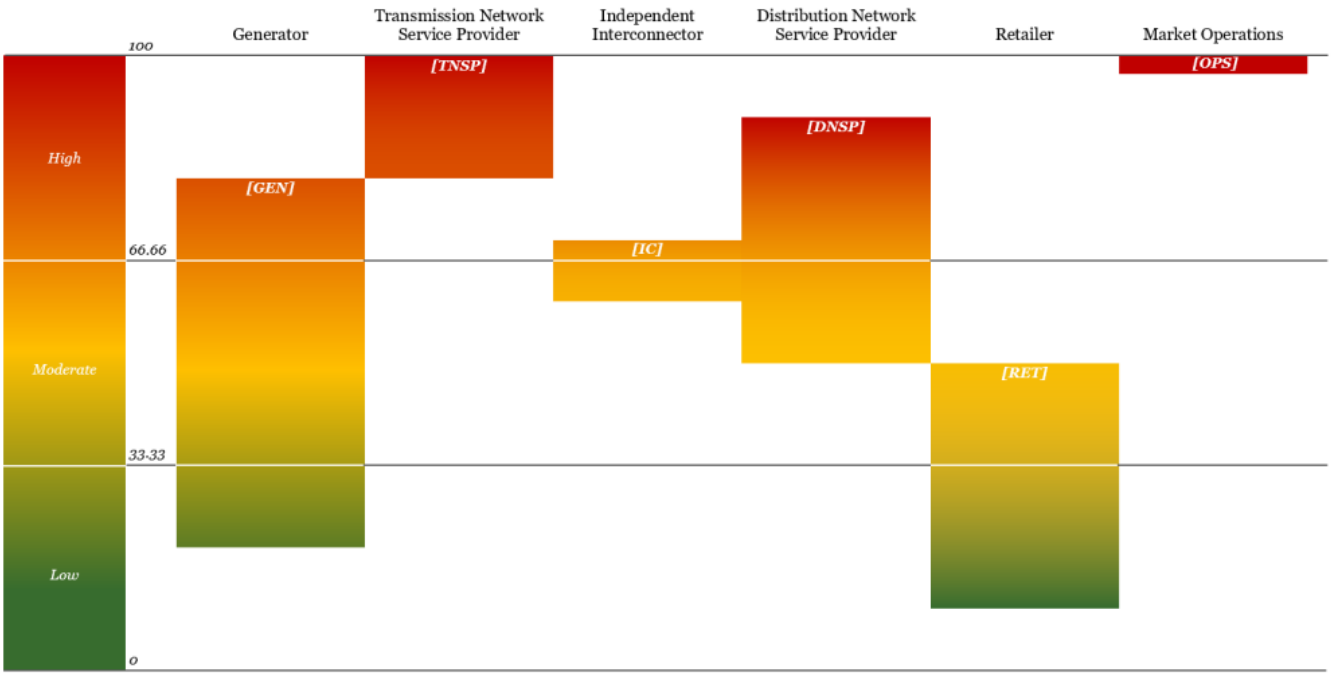
The framework defines cyber security practices across a number of domains and objectives, grouped into three Security Profiles (SPs) defined by the Australian Cyber Security Centre (ACSC) in consultation with AEMO and industry representatives. This tiered risk-based approach ensures that participants target the appropriate maturity level based on their criticality within the energy sector.

The AESCSF provides a consistent baseline on which market participants can develop risk management practices that align with regulatory obligations, including the SOCI Act. By providing a tailored approach to managing cyber risk, the AESCSF strengthens cyber maturity and resilience across the sector.

The following diagram demonstrates the relative criticality of market participants based on their role(s) in the electricity sector. Transmission networks (TNSPs) are now recognised as highly critical components of Australia's energy infrastructure. AusNet's transmission business, among others, is identified as a high-risk asset, underpinning the need for robust cybersecurity measures.

While AESCSF Version 2 does not mandate that market participants achieve certain Security Profiles (SPs) based on their criticality, AEMO's guidance is that organisations should target higher levels of cyber maturity in accordance with their criticality. As a high-criticality market participant, given our role as a Transmission Network Service Provider, AusNet believes it is prudent for us to work towards achieving SP-3 under AESCSF V2 within the TRR 2027-32 regulatory period.

Figure 1 - Criticality Bands by Market Role – AESCSF Electricity Criticality Assessment Tool (E-CAT) 2023 (p5)



1.4.1. How does the framework assess maturity

Maturity Indicator Levels (MILs) are established for each of the 11 domains in the three groups. The MILs assess the maturity of the practices (as levels 0 to 3) measure how well an entity performs within each Domain:

- MIL-0: No formal practices.
- MIL-1: Initial practices exist.
- MIL-2: Practices are documented and repeatable.
- MIL-3: Practices are well-managed and continuously improved.

Security Profiles (SP-1, SP-2, SP-3) represent cyber security maturity levels based on the maturity of an entity's MIL practices across each of the Domains. The SP target level is set based on the entity's criticality, as per Figure 2 above. The SPs are:

- SP-1: For low criticality entities. Basic cyber hygiene and foundational controls.
- SP-2: For medium criticality entities. Intermediate controls and practices.
- SP-3: For high criticality entities. Advanced, robust cyber security practices.

Each SP includes a set of Practices (what should be done) and Anti-Patterns (what should be avoided), spread across 11 Domains. To achieve a given SP, an entity must meet all practices and avoid all anti-patterns for that SP and all preceding SPs across all Domains.

For example, for SP-1 the organisation must meet all practices across all domains to MIL level 1, plus some practices to a level of MIL2 and MIL3. That means that the organisation must be very mature in some areas but can be less mature in others. All MIL requirements must be met for SP1 before it can progress to SP2. The SP score is calculated as a ratio of all the MIL practices achieved for the SP level divided by the total number of MIL practices that are assessed.

1.4.2. Changes to the maturity levels

In 2023, AEMO updated the AESCSF to Version 2 to align with current international standards, and to address emerging technologies and the evolving cyber threat landscape. AusNet has chosen to adopt this updated version. There are now 354 practices that must be met to achieved SP-3, which is 72 more than under version 1 of the AESCSF.

Compared to Version 1, a number of practices were combined or removed and there were an additional 75 practices added.

Table 4 – AESCSF changes – version 1 compared to version 2

	AESCSF v1				AESCSF v2			
	MIL-1	MIL-2	MIL-3	Total	MIL-1	MIL-2	MIL-3	Total
SP-1	57	27	4	88	62 (+5)	57 (+30)	4 (0)	123 (+35)
SP-2	0	94	18	200 (112 + 88)	0	123 (+29)	29 (+11)	275 (152+123) (+40)
SP-3	0	0	82	282 (82 + 200)	0	0	79 (-3)	354 (79+275) (-3)

1.5. Current state of Maturity

AusNet currently holds a level of SP-2 under version 1 of the AESCSF. However, there were significant changes to the requirements for each SP level under Version 2, as shown in **Table 4** above, which an increase of the number of practices required by 20%.

(C-I-C)

This demonstrates that focusing on maintaining current systems and practices result in a deterioration in the security of the network due to the evolution of threats.

The assessment revealed varying levels of maturity across the 11 key cybersecurity domains is shown in **Table 5** along with industry averages. (C-I-C).

The current maturity level reflects a historic focus on regulatory compliance (e.g., SOCI and FIRB obligations), which has now transitioned towards proactive risk management. However, the assessment also highlighted AusNet has demonstrated strong collaboration across cyber, OT, HR, legal, and privacy functions, and a positive cybersecurity culture.

However, to meet its strategic goal of achieving SP3 maturity by 2030, AusNet must transition from compliance-driven efforts to a risk-based, adaptive cybersecurity posture. This includes uplifting operational resilience, enhancing governance, and integrating cybersecurity into broader business transformation initiatives.

Table 5 – AusNet's current maturity against AESCEF V2 domains

AusNet Current State per PwC Assessment	
AESCSF Domain	**(C-I-C)**
Risk Management	(C-I-C)
Cybersecurity Program Management	(C-I-C)
Workforce Management	(C-I-C)
Supply Chain & External Dependencies Management	(C-I-C)
Identity & Access Management	(C-I-C)
Event & Incident Response / Continuity	(C-I-C)
Asset, Change & Configuration Management	(C-I-C)
Situational Awareness	(C-I-C)
Threat & Vulnerability Management	(C-I-C)
Australian Privacy Management	(C-I-C)
Cybersecurity Architecture	(C-I-C)
Overall	**(C-I-C)**

Source: AusNet cybersecurity strategy (March 2025)

1.6. Risk assessment

As part of AusNet's Cyber Resilience Strategy, we have undertaken an assessment of our enterprise cyber security risks. This assessment encompassed the cyber security threats outlined above against the AusNet's Enterprise Risk Framework. We identified two material enterprise risks that are above our material risk threshold:

- Cyber attack impacting Operational Technology (OT) systems (C-I-C) that disrupts the flow of electricity.
- Cyber attack impacting Information Technology (IT) systems [(C-I-C)] that leads to compromise of highly sensitive data or disruption of core enterprise services that OT systems depend on.

Each of these enterprise risks is comprised of seven subcomponent causal risks consisting of the below. Each of these causal risks apply to the enterprise OT and IT risks, collectively representing 14 subcomponent ("Level 2") risks as detailed in **Table 6** below. As part of our Cyber Resilience Strategy we are continuing to mature the assessment and management of these subcomponent risks.

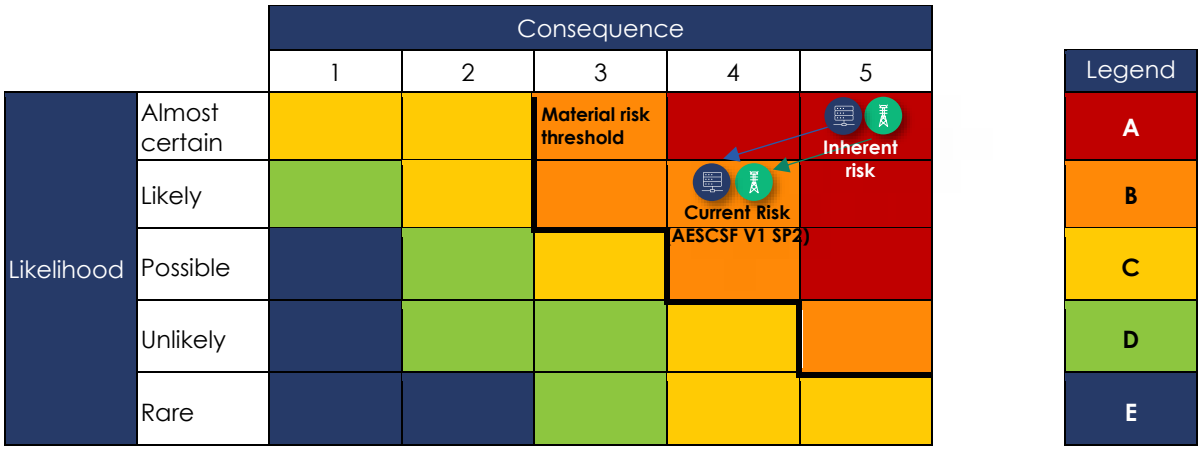
Table 6 Subcomponent causal risks ("Level 2 risks") for OT and IT systems

ENTERPRISE RISKS		CAUSAL RISKS		RISK SCENARIO DESCRIPTION
OPERATIONAL TECHNOLOGY DISRUPTION	INFORMATION TECHNOLOGY DISRUPTUPTION	1	Social engineering/ phishing	Risk of threat actor conducting attacks designed to deceive targets by employing social engineering tactics, to obtain sensitive information or manipulate data and processes
		2	External attack	Risk of threat actor conducting attacks on external infrastructure, including exploiting perimeter vulnerabilities and performing denial-of-service attacks
		3	Data leak/breach	Risk of threat actor conducting attacks that result in the loss, theft and / or compromise of sensitive data (including customer data or sensitive critical infrastructure data), and that cause significant operational, reputational and / or regulatory compliance impacts
		4	Malware/ Ransomware	Risk of threat actor conducting malware-based attacks, including ransomware, that allow the threat actor to disrupt systems, gain control of systems, and leak / exfiltrate sensitive information
		5	Nation-state advanced persistent threat (APT)	A well resourced and motivated state-sponsored threat actor seeks to compromise AusNet's IT for the purposes of espionage, reconnaissance or sabotage. The threat actor may utilise a variety of techniques to achieve an initial foothold in the network, then seek to remain undetected for a long period of time as they exfiltrate sensitive information or plan for a coordinated attack.
		6	Supply chain / 3rd party risk	Risk of threat actor conducting supply chain attacks that result in operational disruption or theft / leakage of sensitive data
		7	Insider threat	Risk of insider threat actor leaking / stealing sensitive information, or disrupting operational systems (either maliciously or inadvertently)

The two enterprise risks have an inherent rating of AusNet's highest risk category (Category A). These risks are assessed as being currently mitigated to Category B by the controls in place to achieve the AESCSF SP2 Version 1 security profile level (refer to Section 1). The inherent risk and current risk levels are shown in **Figure 2Error! Reference source not found.** b elow.

Notably, while current AESCSF SP2 Version 1 level provides a degree of risk reduction, AusNet's current cyber security risk is above our material risk threshold as defined by the Enterprise Risk Management Framework.

Figure 2 – AusNet enterprise Operational Technology (OT) and Information Technology (IT) cyber security risks



Cyber Security Inherent Risk Assessment

	RISK	LIKELIHOOD	CONSEQUENCE	RISK RATING
R1	Cyber attack impacting Operational Technology (OT) systems (e.g., eTerra SCADA) that disrupts the electricity services	Almost certain	5: Significant NEM disruption 5: Public safety / loss of life 5: Reputational damage	A
R2	Cyber attack impacting IT systems (e.g., Active Directory, Communications Network, webMethods integration) that leads to compromise of highly sensitive data or disruption of core enterprise services	Almost certain	5: Significant NEM disruption 5: Reputational damage 5: Regulatory & legal consequences	A

2. Recurrent expenditure

The purpose of this section is to identify the overarching drivers of recurrent capex investment in cyber security for the TRR 2027-32 regulatory period. This investment is focused on maintaining the cyber security systems and applications that were implemented through the RY2022-27 period, to maintain current capabilities.

2.1. Identified needs

As detailed in Section 1, during the FY2022-27 period we have made investments to enhance our cyber security infrastructure, systems and practices across our network businesses. These investments have enabled us to achieve Security Profile 2 (SP-2), as defined in version 1 of the AESCSF.

We have identified that the systems that deliver these capabilities will require refresh during the TRR 2027-32 regulatory period. This recurrent investment relates to updating our existing security appliances, application firewalls, perimeter firewalls, and security information and event management tools. These refreshes will ensure that these systems and applications remain current with latest patches, configurations and vendor support, so as to fully maintain their current level of capability and to maintain our current level of cyber security (AESCSF V1 SP2).

Table 7 summarises the current capabilities that are required to be maintained and the systems currently in place to provide that capability.

Table 7 Summary of current capabilities and systems that will require recurrent expenditure

Capabilities	Summary of systems that provide the capability
Threat Detection and Response	• (C-I-C)
OT/IoT Security	○ (C-I-C)
Cloud Security	• (C-I-C)
Defensible / Zero Trust Architecture	○ (C-I-C)
Identity Access and Management	• (C-I-C)
Cyber Governance and Risk Management	• (C-I-C)

2.2. Options assessment

In developing this business case we have focused on the AER's expectations on the method and approach that should be applied to proposed recurrent ICT expenditure as set out in the AER's guidance note – "Non-network ICT capex assessment approach" of November 2019.

The AER identifies multiple approaches to assess recurrent expenditure. In terms of bottom-up analysis, the AER recognises that recurrent expenditure relates to maintaining an existing service and that it will not always be the case that the investment will have a positive NPV. It expects that a business case will consider possible multiple timing and scope options of the investments (to demonstrate prudency) and options for alternative systems and service providers (to demonstrate efficiency).

To give effect to this methodology we used risk-cost analysis to determine the optimal strategy for recurrent expenditure on cyber security spend categories. Option 1 was to actively manage without lifecycle refreshes. Option 2 was to refresh our cyber security systems in line with vendor recommendations.

Table 8 – Recurrent expenditure options

OPTION	SUMMARY
Option 1: Actively manage without vendor support	Operate our control, metering and business systems without performing updates, patching or refreshes and actively manage the risks in-house
Option 2: Perform lifecycle refreshes **(Recommended option)**	Where prudent and efficient, performing refreshes, upgrades and patching of cyber security systems in line with vendor recommendations and maintaining vendor support

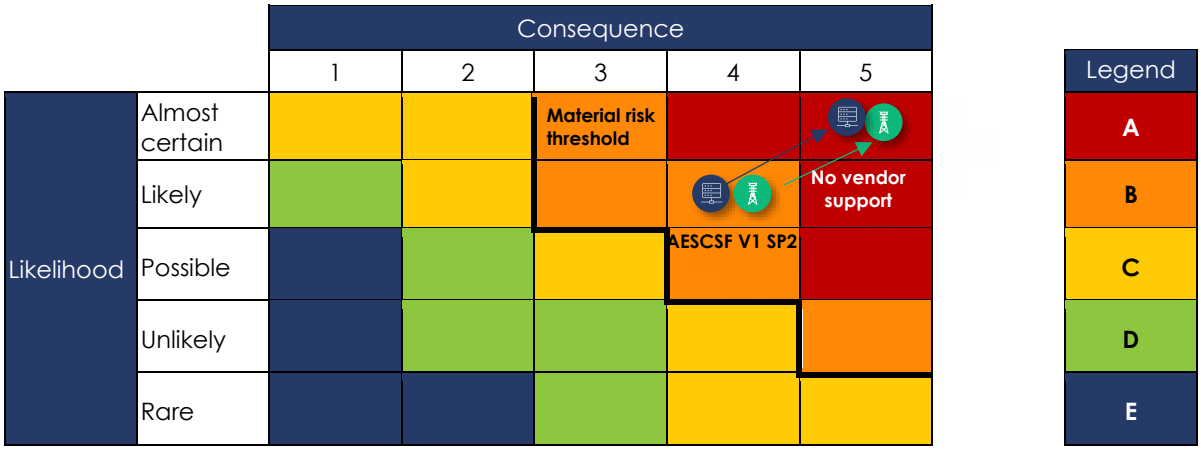
2.2.1. Option 1 – Actively manage without vendor support

Under this option, we would undertake minimal refreshes and seek to actively manage the risks of operating our cyber security systems and applications beyond their expected or recommended cycle. This would effectively operate the systems and applications longer than the recommended refresh period. We would seek to actively manage the risks of systems and applications that present security vulnerabilities or fail in service.

Without vendor support it is likely there will be more unpatched cyber security systems with vulnerabilities, which will see our cyber security environment degrade relative to current capabilities and risk levels. To some degree these can be partly mitigated with additional monitoring, however this would require additional support resources which would result in an opex uplift. If a cyber breach was to occur, it is more likely to spread through these unpatched vulnerabilities increasing the operational consequence of the breach.

The risks associated with this option are shown in **Figure 3**, which reflects degradation of existing cyber controls resulting in cyber security risks elevating to Category A inherent risk level (as described in Section 1.6). We consider that this option will result in an unacceptable elevated risk, particularly as the threat environment evolves and exceeds the capabilities of the existing systems. Therefore, this option does not meet the needs of the business and is not the recommended option.

Figure 3 – Risk Analysis – Risk after adopting Option 1



	RISK	LIKELIHOOD	CONSEQUENCE	RISK RATING
R1.1	Cyber attack impacting Operational Technology (OT) systems (e.g., eTerra SCADA) that disrupts the electricity services	Almost certain	5: Significant NEM disruption 5: Public safety / loss of life 5: Reputational damage	A
R1.2	Cyber attack impacting IT systems (e.g., Active Directory, Communications Network, webMethods integration) that leads to compromise of highly sensitive data or disruption of core enterprise services	Almost certain	5: Significant NEM disruption 5: Reputational damage 5: Regulatory & legal consequences	A

2.2.2. Option 2 – Perform lifecycle refreshes (recommended option)

This option involves refreshing cyber security systems and applications in line with vendor recommendations. This ensures that the systems receive required patching, security and functionality upgrades, and maintain vendor support.

This option sees AusNet maintain the cyber security capabilities that we have implemented in the current period, and maintain our current security profile of SP-2 under AESCSF Version 1. This option is recommended, such that AusNet's capabilities do not degrade. Required recurrent investment to maintain these existing systems is $20.4 million.

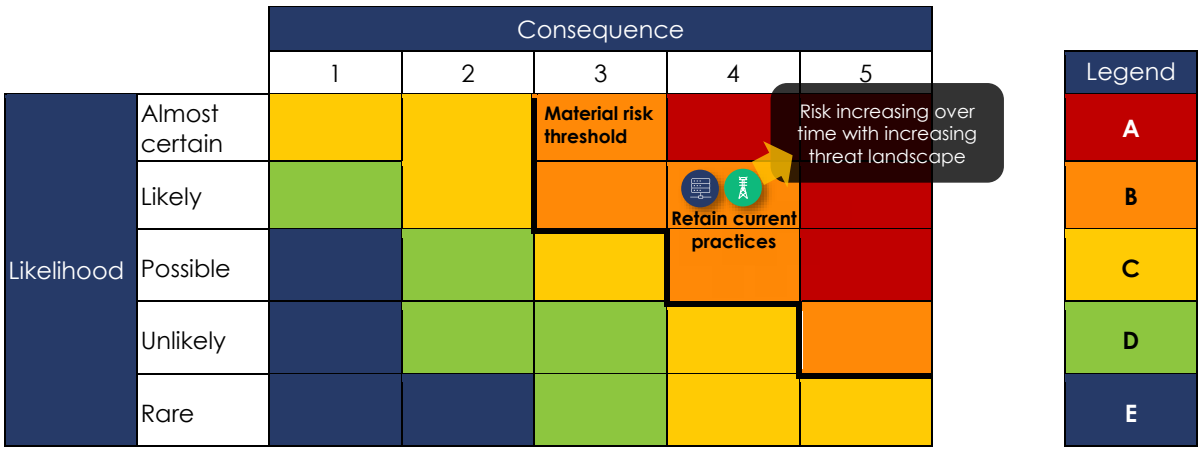
Cost Item	R2028	R2029	R2030	R2031	R2032	Total
Capex	$4.08	$4.08	$4.08	$4.08	$4.08	$20.41
Opex NOTE	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Total	**$4.08**	**$4.08**	**$4.08**	**$4.08**	**$4.08**	**$20.41**

Note: that $0.00m opex implies no increase in expenditure compared to baseline.

However, recurrent investment alone does not enhance AusNet's cyber security posture against the ever-increasing cyber threat landscape. Further non-recurrent expenditure in new capabilities will be required to improve against evolving nature of cyber threats, as detailed in following Section 3. Maintaining current capabilities is a required foundation from which these new capabilities can be built.

This is reflected in Figure 4, which highlights that solely maintaining existing capabilities and SP-2 (Version 1) security posture will result in a progressively deteriorating risk position over time, and AusNet's cyber risks remaining above the material risk threshold.

Figure 4 – Risk Analysis – Risk after adopting Option 2



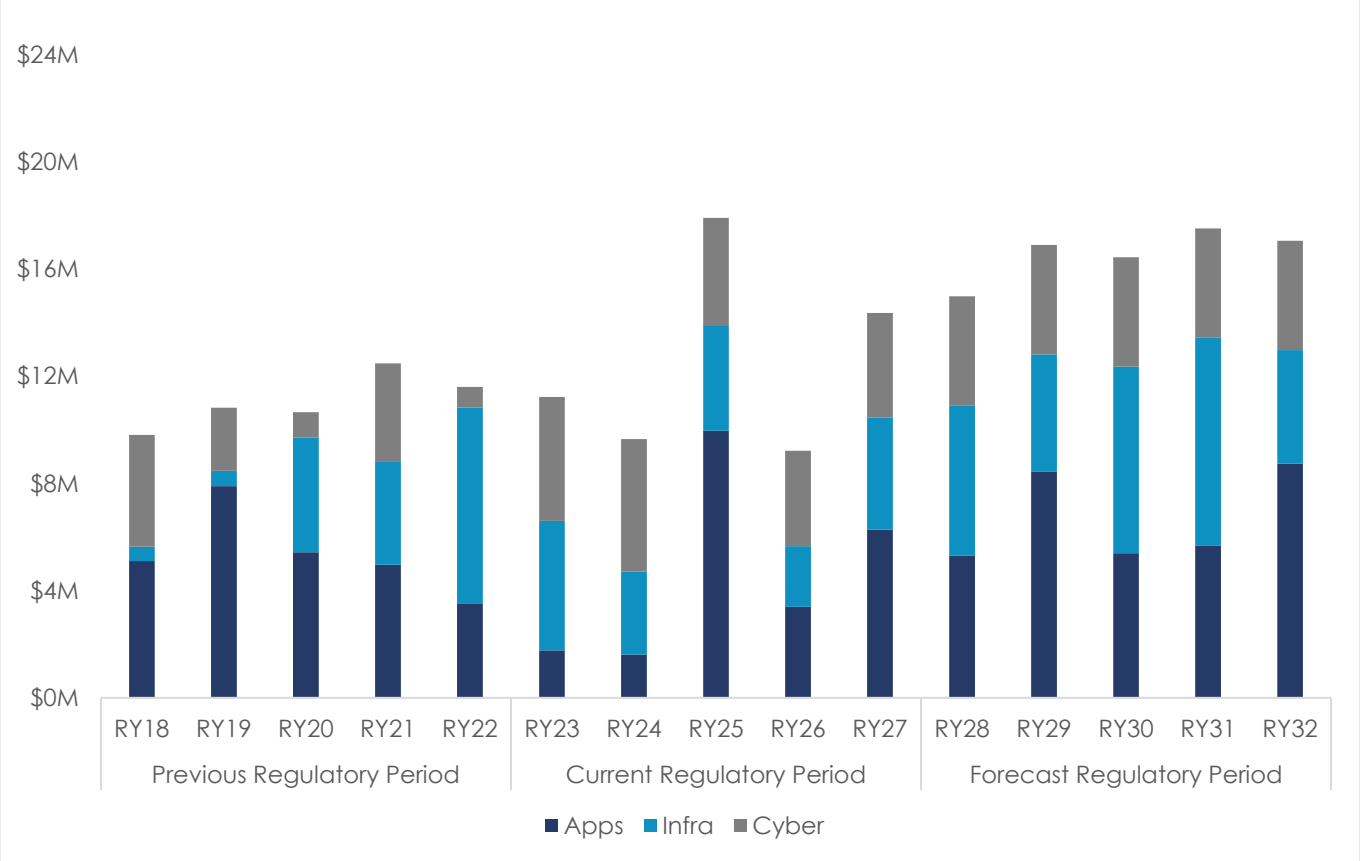
	RISK	LIKELIHOOD	CONSEQUENCE	RISK RATING
R2.1	Cyber attack impacting Operational Technology (OT) systems ((C-I-C)) that disrupts the electricity services	Likely	4: Moderate disruption to the NEM 4: Public safety / loss of life 4: Reputational damage	B
R2.2	Cyber attack impacting IT systems ((C-I-C)) that leads to compromise of highly sensitive data or disruption of core enterprise services	Likely	4: Moderate disruption to the NEM 4: Regulatory & legal consequences 4: Reputational damage	B

2.3. Recommended recurrent expenditure is aligned with historical spend

Figure 5 shows AusNet transmission historical and proposed recurrent digital spend. Expenditure on cyber security is shown by the grey bars and demonstrates that the proposed recurrent expenditure is consistent with the actual historical expenditure during the current regulatory period. The recurrent cyber security expenditure profile is reflective of the periodic lifecycle refreshes and updates required to ensure digital systems remain functional and do not become obsolete as technology, user requirements and security requirement evolve.

The relatively steady level of expenditure demonstrates prudent and efficient management of our existing cyber security capabilities.

Figure 5 – AusNet Transmission Total Recurrent Digital Capex ($m real 2025)



3. Non-recurrent expenditure

The purpose of this section is to detail the drivers of non-recurrent cyber security expenditure for the TRR 2027-32 regulatory period. This investment is focused on uplifting our cyber security capabilities in line with the increasing threat landscape and industry standards.

3.1. Drivers of investment

While we have enhanced our cyber security practices in the current regulatory period, as detailed in Section 1 our current risk and AESCSF security profile highlight that additional investment is required. This demonstrates the need to continue to evolve our capabilities to keep pace with increased cyber threats and associated uplifts in industry standards and best industry practice. The key drivers of cyber security in the TRR 2027-32 period are identified below.

3.1.1. Increased cyber threat

The risk of a cyber attack has significantly increased over the last 5 years. This is due to increased reliance on digital technologies, which are also becoming more inter-connected. There is also a heightened level of cyber threats due to general evolution of cyber malicious activity, and a more disruptive socio-political global environment. There have been a spate of high-profile cyber attacks including:

- Optus – The telecommunications carrier was subject to a cyber attack that resulted in the details of 10,000 customers details being released publicly on the internet.
- Medibank – A cyber attack enabled personal data such as names, addresses, dates of birth, phone numbers, email addresses to be placed on the dark web.
- Qantas – A cyber attack enabled hackers to access personal information for approximately 7 million frequent flyer accounts.

Our intelligence suggests that critical infrastructure providers such as electricity networks continue to be a target of cyber attacks, as described in Section 1. The attack that struck the Ukraine electricity system in 2015 through a series of power outages is a stark reminder of the potential for cyber attacks to have the potential to impact loss of supply. In a more complex geo-political environment, there is increased risk of state sponsored sabotage that directly targets the physical operation of the network.

3.1.2. Change in industry standard on cyber capabilities

It is vital that our cyber security systems and practices continue to keep pace with emerging threats. This has been reflected in Version 2 of the AESCSF released by AEMO in 2023. The Framework was reviewed to align with current international standards and address emerging technologies and the evolving cyber threat landscape. The update demonstrates that capabilities need to continually evolve and new capabilities are required to maintain the same level of security.

As a transmission network services provider, AusNet is classed as a provider of critical infrastructure and consider that it is appropriate to achieve compliance with AESCSF level SP-3 to ensure ongoing secure electricity supply for our customers.

3.1.3. Inter-relationship with customer energy resources

A key driver of improved cyber security is the increasingly complex inter-relationship between our physical network and customer energy resources (CER) including solar and electric vehicles. This means that cyber security needs to consider intrusion entry points from CER, and must also consider the consequential impact to customer devices from attacks on our physical infrastructure.

While the transmission network does not have any CER, we operate as an integrated business with our distribution network and therefore are indirectly exposed to these risks.

Our cyber security strategy takes a holistic approach to the entire business and all service lines, with appropriate cost allocation between the business according to our Cost Allocation Methodology (CAM). This business case only describes the costs directly associated with the transmission business after the CAM has been applied.

3.2. Identified need

In 2025 AusNet completed a Cyber Resilience Strategy, supported by PwC. Section 1.5 summaries the outcomes of the assessment and shows that we are not currently at a level of maturity that is considered industry best practice nor at a level of maturity that is appropriate for a transmission network operator.

The Cyber Resilience Strategy identified a number of capability gaps that AusNet needs to address. These are detailed in Table 9 below. Non-recurrent expenditure in new capabilities is required to mature our cyber capabilities, to address our identified risks and progress from an SP2 level under version 1 of the AESCSF to an SP3 level under version 2 of the AESCSF. This is due to:

- Increased risk of cyber attacks which makes it prudent as an electricity network operator to achieve the highest maturity rating under the AESCSF.
- We expect that the maturity level of V2 SP-3 will become a requirement for providers of critical infrastructure.
- This aligns with our cyber security risk framework which adopts the lowest risk tolerance for cyber security.

The key focus areas for AusNet to uplift to V2 SP3 levels, relative to the identified capability gaps, are described in **Table 9** below.

Table 9 – Identified gaps in capability to meet SP3 level

#	Capability	Description required change
(C-I-C)	**(C-I-C)**	• (C-I-C)
(C-I-C)	**(C-I-C)**	• (C-I-C)
(C-I-C)	**(C-I-C)**	• (C-I-C)
(C-I-C)	**(C-I-C)**	• (C-I-C)
(C-I-C)	**(C-I-C)**	• (C-I-C)
(C-I-C)	**(C-I-C)**	• (C-I-C)
(C-I-C)	**(C-I-C)**	• (C-I-C)
(C-I-C)	**(C-I-C)**	• (C-I-C)
(C-I-C)	**(C-I-C)**	• (C-I-C)
(C-I-C)	**(C-I-C)**	• (C-I-C)
(C-I-C)	**(C-I-C)**	• (C-I-C)

3.3. Options assessment

In developing this business case for the non-recurrent element of cyber security, we have focused on the AER's expectations on the method and approach that should be applied to proposed non-recurrent ICT expenditure as set out in the AER's guidance note – "Non-network ICT capex assessment approach" of November 2019. The AER expects that networks will evidence the need and demonstrate prudency and efficiency of the investment. it is expected that options of scope and timing (to demonstrate prudency) and options for alternative implementation approaches (to demonstrate efficiency) will be evaluated.

As per the AER guidelines, we have examined credible options for our cyber capability maturity, with assessment relative to residual risk and cost to implement. We identified and assessed two credible options for target state maturity levels (Security Profiles) by the end of the TRR 2027-32 regulatory period. These are shown in **Table 10** below.

Table 10 – Non-recurrent expenditure options

OPTION	SUMMARY
Option 1 – Achieve AESCSF Version 2 Security Profile 2	We would invest to only achieve the updated capabilities for SP2 under version 2 of the AESCSF by the end of the TRR 2027-32 regulatory period
Option 2 – Achieve AESCSF Version 2 Security Profile 3	We would invest to achieve the updated capabilities for SP3 under version 2 of the AESCSF by the end of the TRR 2027-32 regulatory period.

3.3.1. Non-credible options

Our options analysis found that maintaining our current level of maturity is not a credible option as the threat landscape is evolving and maintaining current maturity (existing systems and practices) is not aligned with best industry practice and will expose AusNet and its customers to unacceptable risk.

Key disadvantages of only maintaining current systems and practices include:

- Both of the material enterprise risks related to IT and OT will remain above AusNet's material risk threshold.
- It does not reduce any of the 14 causal risks that underpin the two enterprise risks.
- It does not achieve a level of security that AusNet considers is appropriate for critical infrastructure that has been identified as High risk in the AESCSF.
- Limits enablement of AusNet's broader business roadmap.

3.3.2. Option 1 – Achieve AESCSF Version 2 Security Profile 2

Under this option, AusNet will develop programs to address all the gaps in our cyber security environment that have been identified between the current state (AESCSF V1 SP2, (C-I-C)) and the objective of achieving AESCSF V2 SP-2. This would see AusNet meet the 275 AESCSF practices required to reach V2 SP-2 (as compared with 354 practices required to reach SP-3), which includes 75 new practices identified as part of the upgrade of AESCSF Version 1 to Version 2.

The total cost required to uplift our cyber security to meet these V2 SP-2 capabilities over the TRR 2027-32 regulatory period would be $27.03 million capex and $14.04 million opex, representing the transmission network allocation of investments.

Cost item	R2028	R2029	R2030	R2031	R2032	Total
Non recurrent capex	5.41	5.41	5.41	5.41	5.41	27.03
Opex NOTE	2.81	2.81	2.81	2.81	2.81	14.04
Total	**8.23**	**8.23**	**8.23**	**8.23**	**8.23**	**41.07**

Note: This opex is new recurrent opex that is associated with the new systems and practices implemented under non-recurrent capex.

Benefits of this option include:

- Lower investment, consistent with reduced number of systems and practices that need to be addressed (275 for SP-2 vs 354 for SP-3)
- Mitigates 6 to 8 of the 14 causal (Level-2) risks, primarily in IT domains.
- Achieves AESCSF SP2 maturity (v2) which is an improvement from the current maturity level.
- Enables delivery of business transformation initiatives with improved cyber security.

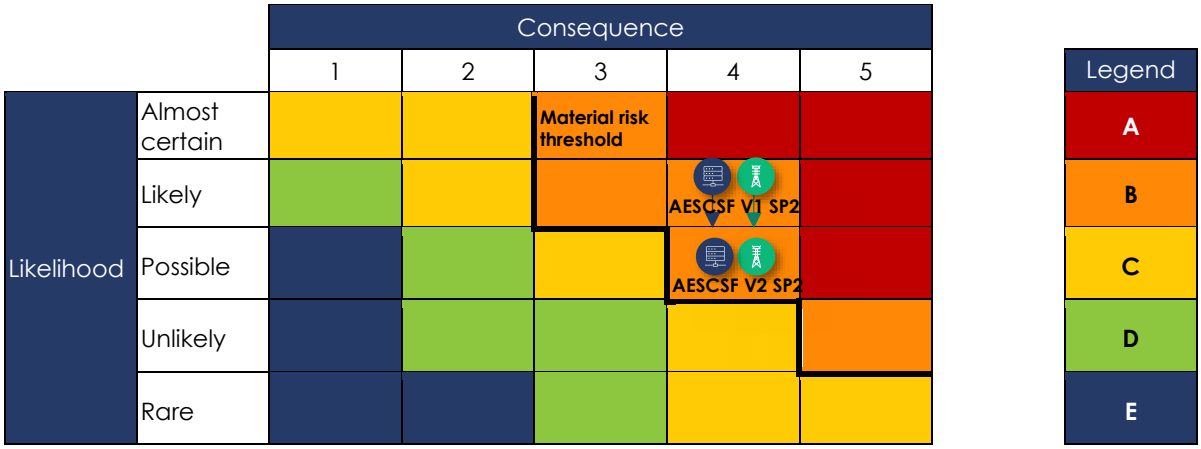
Key residual risks of this option include:

- The resultant security profile is not consistent with industry best practice for critical infrastructure that is classified as high risk under the AESCSF.
- 6 to 8 of the causal (Level 2) risks are not addressed and the overall enterprise OT and IT risks remain above AusNet's Material Risk threshold.
- Will likely leave areas of AusNet exposed to cyber threats, particularly as the threats evolve and our systems and practices are unable to keep up with the lower level of investment.
- (C-I-C)

This option predominately addresses IT risk and does not materially affect OT risks due to the initiatives planned to address the Practices and Anti Patterns set out in the AESCEF V2 for SP2. While the maturity level would be improved compared to the current level, not all identified gaps will be fully addressed when compared to achieving SP3 V2. As discussed in section 1.2, the risk of cyber attack in the current threat environment is far higher than 5 years ago and is likely to increase between now and the end of the next regulatory period.

Figure 6 shows the outcomes of our risk analysis based on achieving SP2 V2 in the upcoming regulatory period. Our risk assessment found that the likelihood will reduce, but the consequence will remain the same. This risk level remains above our Material Risk Threshold and is therefore not acceptable. As a result, AusNet and Victorian customers remain exposed to an elevated level of risk under this option.

Figure 6 - Risk Analysis – Option 1 to achieve AESCSF v2 SP-2 (forecast at end of TRR 2027-32 regulatory period)



	RISK	LIKELIHOOD	CONSEQUENCE	RISK RATING
R1.1	Cyber attack impacting Operational Technology (OT) systems (C-I-C) that disrupts the electricity services	Likely	4: Moderate disruption to the NEM 4: Public safety / loss of life 4: Reputational damage	B
R1.2	Cyber attack impacting IT systems (e.g., (C-I-C)) that leads to compromise of highly sensitive data or disruption of core enterprise services	Likely	4: Moderate disruption to the NEM 4: Regulatory & legal consequences 4: Reputational damage	B

3.3.3. Option 2 – Achieve AESCSF Version 2 Security Profile 3

Under this option, AusNet will develop programs to address all the gaps in our cyber security environment that have been identified between the current state (AESCSF V1 SP2, (C-I-C)) and the objective of achieving AESCSF V2 SP-3. This would see AusNet meet all 354 AESCSF practices required to reach SP-3.

The total cost required to uplift our cyber security to meet these V2 SP-3 capabilities over the TRR 2027-32 regulatory period would be $34.65m capex and $18 million opex, representing the transmission network allocation of investments. Appendix A sets out the detailed program scopes, costs allocated to transmission and total business costs. The forecast costs of this option are consistent with the recommendations from PwC as part of the Cyber Resilience Strategy development and benchmarking.

Cost item	R2028	R2029	R2030	R2031	R2032	Total
Capex	6.93	6.93	6.93	6.93	6.93	34.65
Opex NOTE	3.60	3.60	3.60	3.60	3.60	18.00
Total	**10.53**	**10.53**	**10.53**	**10.53**	**10.53**	**52.65**

Note: This opex is new recurrent opex that is associated with the new systems implemented under non-recurrent capex.

Benefits of this option include:

- Reduces all 14 causal (Level 2) risks, and hence mitigating AusNet's two enterprise cyber security risks to below the material threshold. This includes reduction of the likelihood of a successful cyber event and also the impact of an event as it will be more difficult to propagate through systems.
- Achieves AESCSF SP3 maturity (v2) which is consistent with industry best practice for critical infrastructure that is classified as high risk under the AESCSF.
- Aligns with NIST CMMI 3.5–4.5, (C-I-C).
- Enables a sustainable, adaptive cybersecurity capability across IT and OT.

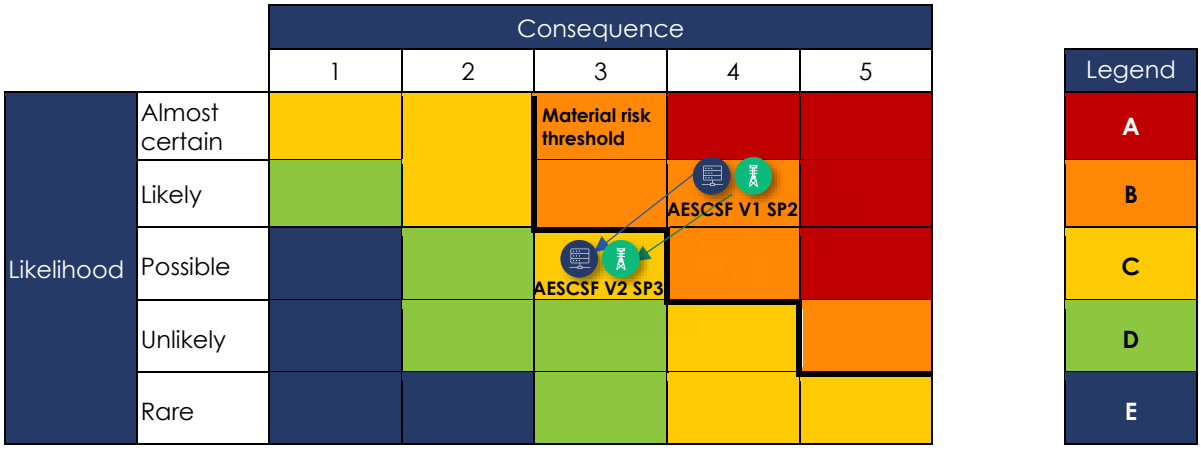
Key residual risks of this option include:

- High organisational dependency and complexity.
- Requires significant uplift in people, processes, and technology.

Figure 7 shows that the programs are focused on reducing the risks relative to Option 1 and to achieve a risk level as low as reasonably practical at the end of the TRR 2027-32 regulatory period.

While the costs Option 2 are higher than option 1, AusNet considers that the reduction in overall risks is significant and as result this option is recommended. Under this option, we would have a comprehensive program that addresses all the identified needs in Sections 3.1 and 3.2. This option would enable AusNet to establish the systems and practices required to manage threats as they evolve within the cyber threat landscape, and to maintain the risk to AusNet within the enterprise material risk threshold.

Figure 7 – Risk Analysis – Option 2 to achieve AESCSF v2 SP-3 (forecast at end of TRR 2027-32 regulatory period)



	RISK	LIKELIHOOD	CONSEQUENCE	RISK RATING
R2.1	Cyber attack impacting Operational Technology (OT) systems (C-I-C) that disrupts the electricity services	Possible	3: Moderate disruption to the NEM 3: Public safety / loss of life 3: Reputational damage	C
R2.2	Cyber attack impacting IT systems (C-I-C) that leads to compromise of highly sensitive data or disruption of core enterprise services	Possible	3: Moderate disruption to the NEM 3: Regulatory & legal consequences 3: Reputational damage	C

NOTE: improved cyber security will reduce the likelihood of a cyber security event and also how far it can propagate through our systems, hence the reduction in both likelihood and consequence under this option.

4. Recommended option

Sections 2 and 3 describe the components of the potential investments that could be undertaken by AusNet to manage our cyber security risks. Recurrent and non-recurrent expenditure are explained separately to simplify the analysis and ensure the drivers and outcomes are clear. However, these are related as new capabilities delivered through non-recurrent expenditure (Section 3) build from those already in place and maintained via recurrent expenditure (Section 2).

The four possible combinations are set out in **Table 11**, noting that it is not credible to undertake non-recurrent expenditure without maintaining existing systems.

Table 11 – Potential combination of recurrent and non recurrent investment options

#	OPTION COMBINATIONS	CAPEX	OPEX	RISK ASSESSMENT
1	Recurrent Option 1 only	-	-	Results in increased risk of business-wide disruption from cyber intrusion
2	Recurrent Option 2 only	$20.41m	-	Degradation of risk position as today's capabilities don't address the evolving cyber threat landscape.
3	Recurrent Option 2 and Non-recurrent Option 1	$47.44m	$14.04m	Improve cyber maturity and reduces the probability of cyber events occurring but does not address the consequence. Does not meet best industry practice or AESCSF recommended maturity level.
4	Recurrent Option 2 and Non-recurrent Option 2	$55.06m	$18.0m	Reduces the probability and consequence of cyber events occurring. Achieves best industry practice and AESCSF recommended maturity level.

Based on assessment of the risk mitigation outcomes, Option 4 is recommended. Per **Table 12** below, this is the only option that mitigates cyber security risks below AusNet's Material Risk threshold.

Table 12 – Options assessment

Criteria	Option 1	Option 2	Option 3	Option 4
Expenditure	**Recurrent only**		**Recurrent and Non-recurrent**	
Capex ($'million, real FY2025)	-	$20.41	$47.44	$55.06
Opex ($'million, real FY2025)	-	-	$14.04	$18.00
Deliverable within timeframe	✓	✓	✓	✓
Reduces risks below Material Risk threshold	×	×	×	✓
AESCSF security profile	Degraded	SP-2 (v1)	SP-2 (v2)	SP-3 (v2)
Preferred option	×	×	×	✓

This recommended option sees AusNet achieve AEMO AESCSF Version 2 Security Profile 3 through the proposal period. Achieving this target state will require:

- Recurrent capex investment of $20.41 million to perform lifecycle refreshes on our current cyber security systems and applications, as detailed in Section 2 Option 2, to maintain our current capability baseline.
- Non-recurrent capex of $34.65m to ensure we comply with 354 practices across our businesses to provide the capability uplift required for AEMO version 2 SP-3.
- New recurrent opex of $18.00 million to manage the new systems, staff, processes and practices implemented.

The total required expenditure in the TRR 2027-32 regulatory period is shown in Error! Reference source not found. below. T hese costs reflect application of AusNet's Cost Allocation Methodology for fair allocation across AusNet's multiple network businesses.

Table 13 – Annual expenditure required for cyber security ($million, real 2025, transmission network cost allocation)

Cost item	R2028	R2029	R2030	R2031	R2032	Total
Recurrent capex *Maintaining AESCSF V1 SP2*	4.08	4.08	4.08	4.08	4.08	**20.41**
Non recurrent capex *Achieving AESCSF V2 SP3*	6.93	6.93	6.93	6.93	6.93	**34.65**
Recurrent opex *Maintaining AESCSF V2 SP3*	3.60	3.60	3.60	3.60	3.60	**18.00**
Total	**14.61**	**14.61**	**14.61**	**14.61**	**14.61**	**73.06**

These recommended options align with the AEMO AESCSF Version 2 expectations consistent with AusNet's market role in transmission. This recommended option:

- Enables AusNet to remain compliant with our obligations under the NER and our Transmission licence requirements;
- Achieves an appropriate level of cyber security based on transmission being high criticality infrastructure based on the AESCSF Electricity Criticality Assessment Tool (E-CAT) 2023;
- Minimises cyber security risk across the organisation as far as reasonably practicable and to within AusNet's materiality risk threshold, and;
- Result in a consistent and optimised cyber security capability for the organisation across all market roles.

A. Non-recurrent expenditure detail

Table 14 sets out the programs of non-recurrent investment to address the identified gaps in capabilities required to meet Security Profile 3, as per AESCSF Version 2, practices by the end of the TRR 2027-32 regulatory period.

We note that program costs have been updated from those included our January 2025 EDPR submission. This is reflective of our ongoing assessment of the transmission system cyber security requirements and the enhancements to AusNet's Cyber Resilience Strategy and roadmap completed through 2025. While total program costs have been adjusted, proposed cost allocation to the distribution business (and resulting EDPR proposal) has not been impacted.

Table 14 – Summary of cyber security initiatives

Program / Initiative	Description	Gaps Addressed (Section 3.2; Table 9)	Total capital cost ($m)	Transmission Allocation ($m)
(C-I-C)	(C-I-C)	(C-I-C)	(C-I-C)	(C-I-C)
(C-I-C)	(C-I-C)	(C-I-C)	(C-I-C)	(C-I-C)

Program / Initiative	Description	Gaps Addressed (Section 3.2; Table 9)	Total capital cost ($m)	Transmission Allocation ($m)
(C-I-C)	(C-I-C)	(C-I-C)	(C-I-C)	(C-I-C)
(C-I-C)	(C-I-C)	(C-I-C)	(C-I-C)	(C-I-C)

Program / Initiative	Description	Gaps Addressed (Section 3.2; Table 9)	Total capital cost ($m)	Transmission Allocation ($m)
(C-I-C)	**[C-I-C]**	(C-I-C)	(C-I-C)	(C-I-C)

Program / Initiative	Description	Gaps Addressed (Section 3.2; Table 9)	Total capital cost ($m)	Transmission Allocation ($m)
(C-I-C)	(C-I-C)	(C-I-C)	(C-I-C)	(C-I-C)
(C-I-C)	(C-I-C)	(C-I-C)	(C-I-C)	(C-I-C)

Program / Initiative	Description	Gaps Addressed (Section 3.2; Table 9)	Total capital cost ($m)	Transmission Allocation ($m)
(C-I-C)	(C-I-C)	(C-I-C)	(C-I-C)	(C-I-C)
(C-I-C)	(C-I-C)	(C-I-C)	(C-I-C)	(C-I-C)
Total			**$54.4m**	**$34.4m**

AusNet

AusNet

Level 31
2 Southbank Boulevard
Southbank VIC 3006

T 1300 360 795

Locked Bag 14051
Melbourne City Mail Centre
Melbourne VIC 8001

Follow us on

@AusNet.Energy
@AusNet

ausnet.com.au