

Electricity Distribution Price Review FY2027 to FY2031 (EDPR 2027-31)

Resubmission Addendum: Cyber Security

Date: 1 December 2025



Table of Contents

Executive Summary	4
1. AusNet's Proposal and AER Draft Decision	5
1.1. Initial Submission Summary	5
1.2. AER Draft Decision feedback	5
2. Cyber Security Risk Mapping	6
2.1. Risk Mapping Overview: Risk Assessment, Causal Scenarios, Required Controls and Current Effectiveness	6
2.2. Current Controls Effectiveness: Information Technology (IT)	8
2.3. Current Controls Effectiveness: Operational Technology (OT)	13
2.4. Required Activity Plan: IT Cyber Security Controls Gaps	18
2.5. Required Activity Plan: OT Cyber Security Controls Gaps	25
2.6. Summary of Required Activity Plan	31
3. Appendix - Acronyms	33

Document history

DATE	VERSION	COMMENT
13/11/2025	V1.0	Draft business case addendum
30/11/2025	V2.0	Final addendum for submission

Related documents

DOCUMENT	VERSION	AUTHOR
Digital Business Case Addendum - Cybersecurity Risk Mapping (Excel)	V2.0	AusNet Services
Revised Proposal Digital Program NPV Model	V2.0	AusNet Services

Approvals

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

Executive Summary

The cyber security program represents AusNet's investment, both recurrent and non-recurrent, to manage cyber security risks in response to heightened cyber threats and evolving regulatory expectations.

AusNet's initial proposal recommended uplifting our capabilities to meet Security Profile 3 maturity under the version 2 of the Australian Energy Sector Cyber Security Framework (AESCSF). This recommendation was based on cost and risk assessment of alternate target maturities, and would see AusNet implementing the most robust controls to mitigate risks as far as reasonably practical, consistent with our assessed risks and criticality under the AESCSF. To reach target Security Profile 3 maturity, AusNet's initial proposal included \$27.5M capex and \$1.8m opex (\$real 2026) for the cybersecurity program.

The AER's Draft Decision accepted the key components of AusNet's cyber security proposal as prudent, specifically:

- Accepting that AusNet has demonstrated the need to achieve higher security level of AESCSF (version 2) Security Profile 3
- Accepting proposed expenditure of \$27.5 million capex and \$1.8m opex (\$real 2026), as a placeholder

However, the AER's Draft Decision provided feedback that AusNet had not provided detailed mapping of the risks faced against the proposed activities and costs needed to address them across our networks.

Since our initial proposal, and addressing the AER's Draft Decision feedback, AusNet has further matured our assessment of our cyber security risks, as part of our Cyber Resilience Strategy developed with engagement from PwC. From this assessment we have consolidated to two material cyber security risks:

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

To fully evaluate our current risk profile, and activities required to reach target state, we have further assessed the seven causal scenarios for each of these two material risks, the required risk mitigation controls and their current effectiveness (based on AusNet's current AESCSF version 1 Security Profile 2 maturity level), and the activity plan required to address control effectiveness gaps. From this assessment, we have revalidated the required activity program, with investment across 9 programs required to address identified gaps and reach AESCSF version 2 Security Profile 3 target state maturity. These investment programs are consistent with those proposed in AusNet's Transmission Revenue Reset.

Through this detailed mapping of cyber security risks, to their required controls and current effectiveness, and to the activities required to address identified control gaps and mitigate risks, AusNet has addressed the AER's Draft Decision feedback. Our revised proposal remains unchanged, with expenditure of \$27.5 million capex and \$1.8m opex (\$real 2026) to reach target state maturity of Security Profile 3 (AESCSF version 2) in the upcoming regulatory period.

1. AusNet's Proposal and AER Draft Decision

The cyber threat landscape is increasingly challenging and complex due to greater digital interconnectivity and the rise of sophisticated attacks, as demonstrated by recent high-profile incidents. As a critical infrastructure provider, AusNet must continually enhance our cyber security measures to safeguard our operations and customers. While our investments to date provide a foundation, ongoing investment to enhance capabilities is essential to address evolving threats, keep pace with updated industry standards, and respond to the Australian Government's strengthened cybersecurity strategy and recent legislative reforms.

This section outlines our proposed cyber security investments and summarises the Australian Energy Regulator's (AER's) Draft Decision, which accepted the key components of AusNet's proposal.

1.1. Initial Submission Summary

AusNet has a complex and integrated suite of technology systems, applications and infrastructure that enable us to deliver an affordable and reliable electricity distribution network service to our customers. Keeping our digital assets secure from cyber threats is fundamental, given the potential for widescale disruption of our electricity services resulting from a successful cyber compromise. Recognising this risk, AusNet has undertaken significant investment in the current FY2021-26 period to achieve a Security Profile 2 (SP-2) maturity under version 1 (v1) of the Australian Energy Sector Cyber Security Framework (AESCFS) published by the Australian Energy Market Operator (AEMO).

AusNet's initial cyber security proposal for the FY2027-31 period identified that cyber security threats have intensified over the past 5 years with a spate of major attacks on businesses in Australia such as Optus and Medibank. Highlighted was the evolution of threat actor capabilities and also geo-political instability that is fuelling the risk of state-sponsored sabotage. In recognition of this evolving threat landscape version 2 of the AESCSF was rolled out in the current regulatory period, raising standards by introducing significant changes designed to align with international best practices and address emerging technologies and evolving cyber threats.

Consistent with this threat landscape, AusNet's initial proposal assessed that the current cyber security risks to our distribution network operations, customer and market data, and corporate compliance and operations, were outside of our risk appetite. This assessment recognised AusNet's role as a multi-network business and high criticality rating per the AESCSF.

The initial proposal assessed multiple options for recurrent expenditure, to maintain existing cyber security systems and capabilities, and non-recurrent expenditure to uplift our current cyber security capabilities. This assessment evaluated the AusNet's risk position in the proposal period from reaching target state maturities of AESCSF version 1 Security Profile 2 (current maturity) to AESCSF version 2 Security Profile 2 (moving to latest industry standard), and AESCSF version 2 Security Profile 3 (reaching highest maturity per latest industry standard).

Based on assessment of the risk and cost of the various options, AusNet recommended targeting AESCSF version 2 Security Profile 3 maturity as prudent, implementing the most robust controls to mitigate risks as far as reasonably practical. AusNet proposed expenditure of \$24.9m capex and \$1.7m opex (\$real 2024) to reach this target maturity, with these amounts representing a 25% allocation of program costs to distribution.

1.2. AER Draft Decision feedback

The AER's Draft Decision accepted the key components of AusNet's cyber security proposal as prudent, specifically:

- Accepting that AusNet has demonstrated the need to achieve higher security level of AESCSF (Version 2) Security Profile 3
- Accepting proposed expenditure of \$27.5 million capex and \$1.8m opex (\$real 2026), as a placeholder

However, in the Draft Decision the AER provided feedback that AusNet had not provided detailed mapping of the risks that it faces against the activities and costs it suggests is needed to address this, across our three regulated networks.

The AER Draft Decision advised that the proposed cyber security program was accepted as a placeholder, with this detailed mapping of the risks, activities, and costs, to business drivers, required in AusNet's Revised Proposal to support the program.

2. Cyber Security Risk Mapping

Through 2025, since our initial proposal, AusNet has further matured our assessment of cyber security risks, including revalidation of key risks, evaluation of causal scenarios, assessment of required controls and their current effectiveness, and the required action plan to address identified gaps. This work has been undertaken as part of our Cyber Resilience Strategy, developed with engagement from PwC.

This detailed risk mapping has confirmed the alignment of AusNet's proposed cyber security enhancements and investment program with closure of identified controls gaps. This detailed risk mapping is provided in support of AusNet's program to address the AER's Draft Decision feedback.

2.1. Risk Mapping Overview: Risk Assessment, Causal Scenarios, Required Controls and Current Effectiveness

Through 2025 AusNet have further matured our assessment of our cyber security profile, as part of our Cyber Resilience Strategy developed with engagement from PwC. This work further has advanced the risk assessment included in AusNet's initial proposal, revalidating our material risks and further assessing causal scenarios, required controls and their current effectiveness.

This assessment encompassed evaluation of the cyber security threats detailed in our initial proposal against AusNet's Enterprise Risk Framework. From this assessment we have consolidated to two material cyber security risks that are above our material risk threshold:

- **Cyber attack impacting Operational Technology (OT) systems** [e.g., SCADA] that disrupts the flow of electricity.
- **Cyber attack impacting Information Technology (IT) systems** [e.g., Customer Systems, System Integration Platforms] that leads to compromise of highly sensitive data or disruption of core enterprise services that OT systems depend on.

Seven causal scenarios have been identified and evaluated for each of these material risks. Details of each of these causal scenarios are provided in **Table 1** below; each of the causal risks apply to the each of the OT and IT material risks.

Table 1 -1 Causal scenarios / threat pathways for OT and IT systems

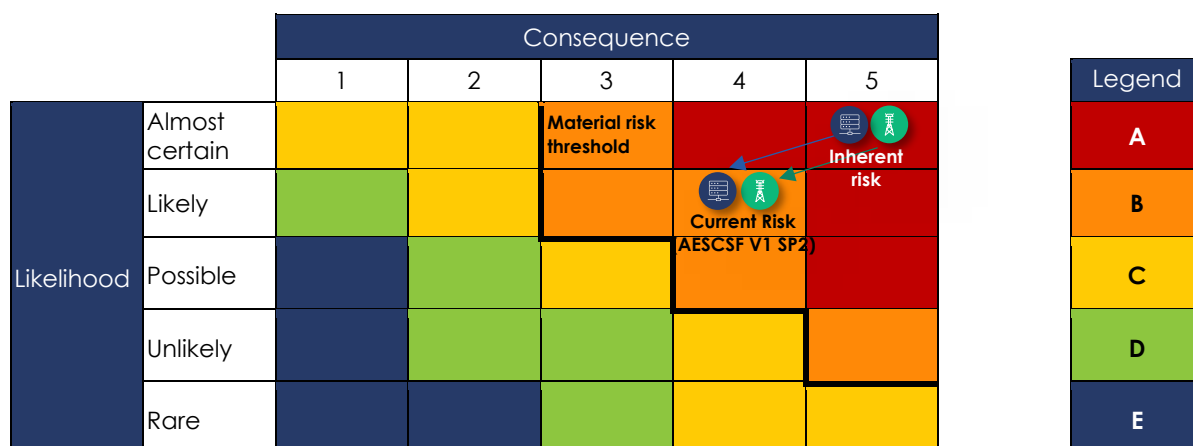
MATERIAL RISKS		CAUSAL SCENARIOS	RISK SCENARIO DESCRIPTION
OPERATIONAL TECHNOLOGY DISRUPTION	INFORMATION TECHNOLOGY DISRUPTION	1 Social engineering / phishing	Risk of threat actor conducting attacks designed to deceive targets by employing social engineering tactics, to obtain sensitive information or 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)

With regard to these causal scenarios, we have revalidated our assessment of the two material OT and IT risks. Each as been assessed to have an inherent rating of AusNet's highest risk category (Category A), as shown and described in **Figure 1** below.



We have further evaluated the required controls, and their current effectiveness, to mitigate these material risks and their causal scenarios. This assessment is detailed in Sections 2.2 and 2.3, and is reflective of AusNet's current AESCSF Version 1 SP2 Security Profile maturity.

Based on this controls effectiveness assessment, our material OT and IT risks are assessed as being currently mitigated to Category B (as shown in in **Figure 1**). Notably, while current AESCSF Version 1 SP2 maturity 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 1 – AusNet Operational Technology (OT) and Information Technology (IT) cyber security risks



Cyber Security Inherent Risk Assessment

	RISK	LIKELIHOOD	CONSEQUENCE	RISK RATING
	OT Risk Cyber attack impacting Operational Technology (OT) systems (e.g., SCADA) that disrupts the electricity services	Almost certain	5: Significant customer supply disruption 5: Public safety / loss of life 5: Reputational damage	A
	IT Risk Cyber attack impacting IT systems (e.g., Customer Systems, System Integration Platforms) that leads to compromise of highly sensitive data or disruption of core enterprise services	Almost certain	5: Significant customer impact 5: Reputational damage 5: Regulatory & legal consequences	A

2.2. Current Controls Effectiveness: Information Technology (IT)

To fully evaluate our current cyber security risk position, and the actions required to reach our target risk mitigation, we have completed detailed assessment of required controls and their current effectiveness relative to each causal risk. This assessment represents the basis of our current risk position, as described in Section 2.1. This assessment further provides the basis for the investment program required in the upcoming regulatory period, in order to address controls effectiveness gaps and reach our target risk mitigation position.

Required controls and their current effectiveness for AusNet's IT cyber security risk are detailed in the table below. This table is additionally provided in the Digital Business Case Addendum - Cybersecurity Risk Mapping (Excel) document in our Revised Proposal.

Table 2 - Control effectiveness: IT controls

ID	Required Controls	Control description	IT Cyber Risk (Scenarios/Causes)							Current Control Effectiveness and Assessment Basis
			Social Engineering	External Attack	Malware/Ransomware	Nation State Sponsored/APT	Supply Chain/3rd Party Risk	Insider Threat	Data Breach	
Access Management										
(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)
(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)	(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)	(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)	(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)	(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)	(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)	(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)	(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)	(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)	(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)

Legend

Yes	
No	
Partially Effective	
Ineffective	
Effective	

2.3. Current Controls Effectiveness: Operational Technology (OT)

As per IT cyber security risk, required controls and current status of effectiveness has been evaluated for AusNet's OT cyber security risk. Assessment is detailed in the table below and additionally provided in the Digital Business Case Addendum - Cybersecurity Risk Mapping (Excel) document in our Revised Proposal.

Table 3 - Control effectiveness: OT controls

ID	Required Controls	Control description	OT Cyber Risk (Scenarios/Causes)							Current Control Effectiveness and Assessment Basis
			Social Engineering	External Attack	Malware/ Ransomware	Nation State Sponsored/APT	Supply Chain/ 3rd Party Risk	Insider Threat	Data Breach	
(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)	(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)	(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)	(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)	(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)	(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)	(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)	(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)	(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)	(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)	(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)
(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)	(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)

Legend – As per IT controls and effectiveness assessment

2.4. Required Activity Plan: IT Cyber Security Controls Gaps

Based on our assessment of current controls effectiveness, as detailed in Sections 2.2 and 2.3, our Cyber Resilience Strategy has assessed the activities required to address identified controls deficiencies and reach our target risk position. This is consistent with our proposal basis of reaching AESCSF Version 2 Security Profile 3 level maturity.

The required activities to address IT cyber security controls effectiveness gaps are detailed in the table below. Also referenced is the associated investment program, as were detailed in AusNet's initial proposal, which will deliver the required uplift. This table is additionally provided in the Digital Business Case Addendum - Cybersecurity Risk Mapping (Excel) document in our Revised Proposal.

Table 4 - Action Plan: IT cyber security controls gaps

ID	Required Controls	Control description	Current Control Effectiveness	Required Action Plan to Address Control Effectiveness Gaps	Associated Investment Program		
					Primary	Secondary	
(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)

(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)	(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)	(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)	(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)	(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)	(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)	(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)
---------	---------	---------	---------	---------	---------	---------	---------

2.5. Required Activity Plan: OT Cyber Security Controls Gaps

As per IT cyber security risk, our Cyber Resilience Strategy has assessed the activities required to address OT cyber security controls effectiveness gaps. These required activities, and the associated investment program which will deliver the required uplift, are detailed in the table below. This table is additionally provided in the Digital Business Case Addendum - Cybersecurity Risk Mapping (Excel) document in our Revised Proposal.

Table 2 - Control effectiveness: OT controls

ID	Required Controls	Control description	Current Control Effectiveness	Required Action Plan to Address Control Effectiveness Gaps	Associated Investment Program Primary	Secondary
(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)	(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)
(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)	(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)
(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)	(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)	(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)	(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)

2.6. Summary of Required Activity Plan

Following the comprehensive review of cyber security risks, required controls and effectiveness, we have validated that our required uplift activity plan consists of nine investment programs. This represents an update from the programs detailed in our initial proposal, with addition of required programs for (C-I-C), and removal of (C-I-C). These investment programs are consistent with those detailed in AusNet's recent Transmission Revenue Reset proposal.

The details of each investment program is provided in Table 7 below, along with the identified controls effectiveness gaps the program addresses. Each initiative either directly or indirectly contributes to closing specific identified controls gaps, with many programs interconnected and mutually reinforcing. It is important to note that the number of gaps addressed by each initiative does not necessarily reflect the complexity or investment required; in some cases, larger financial commitments are necessary to address more challenging or foundational issues, even if the gap count appears lower. Overall, the breadth and integration of these programs ensure that all critical areas are targeted, and our approach remains robust and fit for purpose to uplift our security posture and risk management capabilities.

While required activity programs have been revalidated, AusNet is not proposing any change to \$27.5M capex and \$1.8m opex (\$real 2026) initial proposal expenditure.

Table 3 - Control effectiveness: IT controls

ID	Investment Program	Scope	Primary Gap Closure	Secondary Gap Closure
(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)	• (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. Appendix - Acronyms

For Reference - Cyber security acronyms used in this document

- SoD - Segregation of Duties
- PAM - Privileged Access Management
- RTO/RPO - Recovery time objective/Recovery Point objective
- SOC - Security Operations Centre
- TPRM - Third Party Risk Management
- EoL / EoS – End of Life / End of Support
- WAF – Web Application Firewall
- DLP – Data Loss Prevention
- TI – Threat Intelligence
- PLC – Programmable Logic Controller
- RTU – Remote Terminal Unit
- NGFWs – Next-Generation Firewalls
- SBOMs – Software Bill of Materials
- ICS – Industrial Control System
- SOEs – Standard Operating Environments
- RBAC – Role-Based Access Control
- HMI – Human-Machine Interface
- OT – Operational Technology
- PKI – Public Key Infrastructure

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

