

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

Resubmission Addendum: Technology Asset Management - Infrastructure

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. AusNet's Revised Proposal	6
2.1. Enhanced approach to managing digital resilience risk	6
2.2. System criticality and revalidation of upgrade timing drivers	8
2.3. Upgrade costs and Distribution allocations	9
3. Evaluation of Options	12
3.1. Option 1 – Proactive refreshes on Mission Critical infrastructure only	12
3.2. Option 2 – Proactive refreshes on Mission and Business Critical infrastructure only	13
3.3. Option 3 – Proactive lifecycle refreshes for all infrastructure	14
3.4. Recommended option	15

Document history

DATE	VERSION	COMMENT
12/11/2025	V1.0	Draft business case addendum
28/11/2025	V2.0	Final addendum for submission

Related documents

DOCUMENT	VERSION	AUTHOR
Wipro - Cost Estimation Report	V1.0	Wipro
Revised Proposal Digital Program NPV Model	V2.0	AusNet Services

Approvals

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

Executive Summary

Technology Asset Management (TAM) represents AusNet's recurrent expenditure to maintain the resilience and existing capabilities of the technology infrastructure that enables us to deliver an affordable and reliable distribution network service to our customers. Through this program AusNet applies a risk-based refresh approach to maintain our data centres and communications, consistent with our risk management policies.

The AER's Draft Decision did not approve AusNet's initial proposal for TAM Applications, with alternative capex forecast detailed in **Table 1** below.

Table 1 - AER Alternative Forecast Expenditure (\$m, real FY2026)

Cost item	Initial Proposal	AER Alternative	Adjustment
Capex	\$32.7M	\$17.2M	-47%
Opex	-	-	-

The AER details reasons for the Draft Decision adjustments, which AusNet has addressed in our Revised Proposal:

AER Draft Decision Feedback	How this has been addressed in AusNet's Revised Proposal
Not considering a prudent option of extending lifecycles for some infrastructure on a risk basis	<ul style="list-style-type: none"> Through 2025 AusNet has implemented an enhanced systems criticality and risk management framework, which has been applied for the Revised Proposal to guide our approach to proactive and reactive refreshes Application of this framework has reduced forecast refresh requirements for lowest criticality Business Operational & Administrative infrastructure
Cost estimates not based on referenceable bottom-up assessments, with potential for over-estimation bias	<ul style="list-style-type: none"> AusNet has revalidated cost estimates, incorporating updated project figures since the initial submission, to refine our revised proposal against historical benchmarks Where there were no historical benchmarks available, our digital infrastructure partner (Wipro) has completed cost estimates.
Allocation of costs between AusNet's distribution, transmission and gas network businesses	<ul style="list-style-type: none"> AusNet's initial proposal reflected only distribution network allocated costs, as per our Cost Allocation Methodology. These shared systems allocations have been more clearly documented in our Revised Proposal

In addressing the AER's Draft Decision feedback, AusNet evaluated three options for the Revised Proposal program. These options assessed the relative cost and risk reduction benefit from alternative proactive and reactive approaches to each of our infrastructure criticality categories. The results of this assessment are details in **Table 2**, with the preferred Option 2 providing balance between required expenditure with mitigation of material risks.

Table 2 - Options assessment results (\$m, real 2024, distribution network cost allocation)

#	OPTION NAME	COST (TOTEX \$M)	MITIGATES MATERIAL RISKS	PREFERRED
1	Proactive refreshes on Mission Critical infrastructure only	\$22.2m	No	No
2	Proactive refreshes on Mission & Business Critical infrastructure only	\$25.6m	Yes	Yes
3	Proactive lifecycle refreshes for all infrastructure	\$39.0m	Yes	No

Based on this assessment, AusNet's Technology Asset Management – Infrastructure revised proposal represents \$25.6m capex. All costs represent distribution network allocation. Expenditure profile through the 2026-31 regulatory period is detailed in **Table 3** below, which represents a \$4.0m reduction relative to AusNet's initial proposal.

Table 3 - Forecast expenditure for Option 2 (\$m real 2024, distribution network allocated costs)

Cost item	RY27	RY28	RY29	RY30	RY31	Total
Capex	5.1	4.0	4.7	5.7	6.1	25.6
Opex	-	-	-	-	-	-
Total	5.1	4.0	4.7	5.7	6.1	25.6

1. AusNet's proposal and AER Draft Decision

ICT infrastructure includes compute servers, storage servers, telecommunications and end user devices. Infrastructure is the foundation of the technology systems that enable AusNet to reliably and securely operate our distribution network, plan and maintain our assets, engage with our customers, and efficiently run our business. For this purpose, AusNet owns and operates ICT infrastructure 'on premise' in our Richmond and Rowville data centres, which underpins our distribution network services.

This section summarises AusNet's initial 2026-31 regulatory period proposal for "Technology Asset Management" (TAM): recurrent expenditure to maintain the resilience and existing capabilities of our ICT infrastructure. Also detailed is the Australian Energy Regulator's (AER's) Draft Decision, alternative forecast, reasons for adjustments to AusNet's proposal, and feedback to be addressed in our revised proposal.

1.1. Initial Submission Summary

AusNet's initial submission proposed expenditure to replace end of life hardware, refurbish data centre facilities, replace end of life telecommunications infrastructure, and undertake refresh of end use devices. Expenditure needs in the FY2027-31 regulatory period were identified through a bottom-up assessment of infrastructure systems to determine the known or likely timing of vendor refresh requirements. Cost estimates were developed based on historical benchmarks for similar infrastructure refreshes and through workshop engagement with AusNet's digital partners, and represented cost allocation to the distribution network where systems are shared across AusNet's regulated networks.

Recognising that 'on premises' infrastructure almost entirely underpins critical network operations capabilities, based on assessment of cost and risks the recommended option was to refresh infrastructure in line with vendor recommendations. Proposed expenditure was \$29.6 million capex (\$real 2024), as shown in **Table 4** below.

Table 4 - Initial Submission Forecast Expenditure for Technology Asset Management - Infrastructure (\$m, real FY2024)

Cost item	FY2027	FY2028	FY2029	FY2030	FY2031	Total
Capex	\$6.58M	\$5.90M	\$5.30M	\$5.80M	\$6.02M	\$29.60M
Opex	-	-	-	-	-	-
Total	\$6.58M	\$5.90M	\$5.30M	\$5.80M	\$6.02M	\$29.60M

1.2. AER Draft Decision feedback

The AER did not accept AusNet's proposed expenditure and the Draft Decision included an alternative forecast of \$17.2m capex (\$real 2026), per **Table 5** below.

Table 5 - AER Alternative Forecast Expenditure (\$m, real FY2026)

Cost item	Initial Proposal	AER Alternative	Adjustment
Capex	\$32.7M	\$17.2M	-47%
Opex	-	-	-

The AER Draft Decision, and associated EMCa consultant report, detail three reasons for the adjustment to capex:

- Not considering a prudent option of extending lifecycles for some infrastructure on a risk basis
- Cost estimates not based on referenceable bottom-up assessments, with potential for over-estimation bias. EMCa specifically highlight DERMS and ADMS hardware, which are relatively new systems.
- Allocation of costs between AusNet's distribution, transmission and gas network businesses

2. AusNet's Revised Proposal

In response to the AER's Draft Decision, AusNet has reviewed the Technology Asset Management – Infrastructure program. This section details the approach taken to specifically address the Draft Decision feedback, and the revised proposal changes that have resulted from this review.

2.1. Enhanced approach to managing digital resilience risk

AusNet has always applied a risk-based management approach to maintaining digital infrastructure resiliency through lifecycle upgrades; actively seeking to balance costs relative risks and deferring upgrades where prudent.

Criticality Assessment and Risk Management Framework

Through 2025, we have enhanced our digital criticality assessment and associated risk management framework. This refinement sees digital infrastructure classified into three categories based on the functions it performs and the applications it supports. Each category underpins how resilience and cyber security risks are assessed and managed. The categories also determine whether we adopt a proactive or reactive refresh strategy.

Mission Critical (Proactive) - Infrastructure essential to maintaining electricity supply to our distribution network customers, where failure could cause significant and sustained disruption.

- Example: Servers supporting the SCADA system, where loss of functionality could prevent network control.
- Approach: Proactively refresh infrastructure before the end of extended vendor support with a bias towards refreshing earlier than business critical systems to keep material risk within threshold for these most critical systems.

Business Critical (Proactive) - Infrastructure supporting enterprise-wide business applications, where failure could cause material business disruption, regulatory exposure, reputational harm, or substantial cost impacts.

- Example: Core business application servers.
- Approach: Proactively refresh infrastructure before the end of extended vendor support to minimise risk as far as reasonably practicable level.

Business Operational and Administrative (Reactive) - Infrastructure that supports day-to-day operations but does not pose material risks to network operations or business continuity.

- Example: User devices such as laptops and desktop computers.
- Approach: Manage upgrades reactively by replacing assets when performance issues or cyber vulnerabilities arise.
- Note: This approach may extend upgrade cycles beyond vendor recommendations, but identified vulnerabilities are remediated promptly to prevent intrusion via weak points. Cyber security considerations can therefore become the primary driver for upgrades in this category.

Infrastructure Asset Lifecycle Management

AusNet's infrastructure lifecycle management approach balances functionality, cost, and resilience. We assess not only whether an asset continues to operate, but also the risks and consequences of failure, including the speed of recovery and the availability of security patches to manage emerging cyber threats.

Our lifecycle management considers three key phases of vendor support:

- 1. Vendor Mainstream Support** - Assets are fully supported with access to spares, security patches, and warranty coverage.
 - Failures can be resolved rapidly.
 - Aligns with our proactive refresh strategy—assets are replaced before mainstream support ends.
- 2. Vendor Extended Support** - Support is more limited, with reduced access to spares and longer response times.
 - The likelihood of failure increases as assets age.
 - AusNet typically refreshes infrastructure before this phase concludes, maintaining acceptable risk levels.

3. End of Support - Vendor support, patches, and spares are no longer available.

- Failures take longer to resolve, often relying on internal or secondary markets for components.
- Cyber vulnerabilities may remain unpatched.
- This phase is reserved for low-risk, non-critical assets such as laptops or passive hardware (e.g. racks).

Preferred Lifecycle Strategy

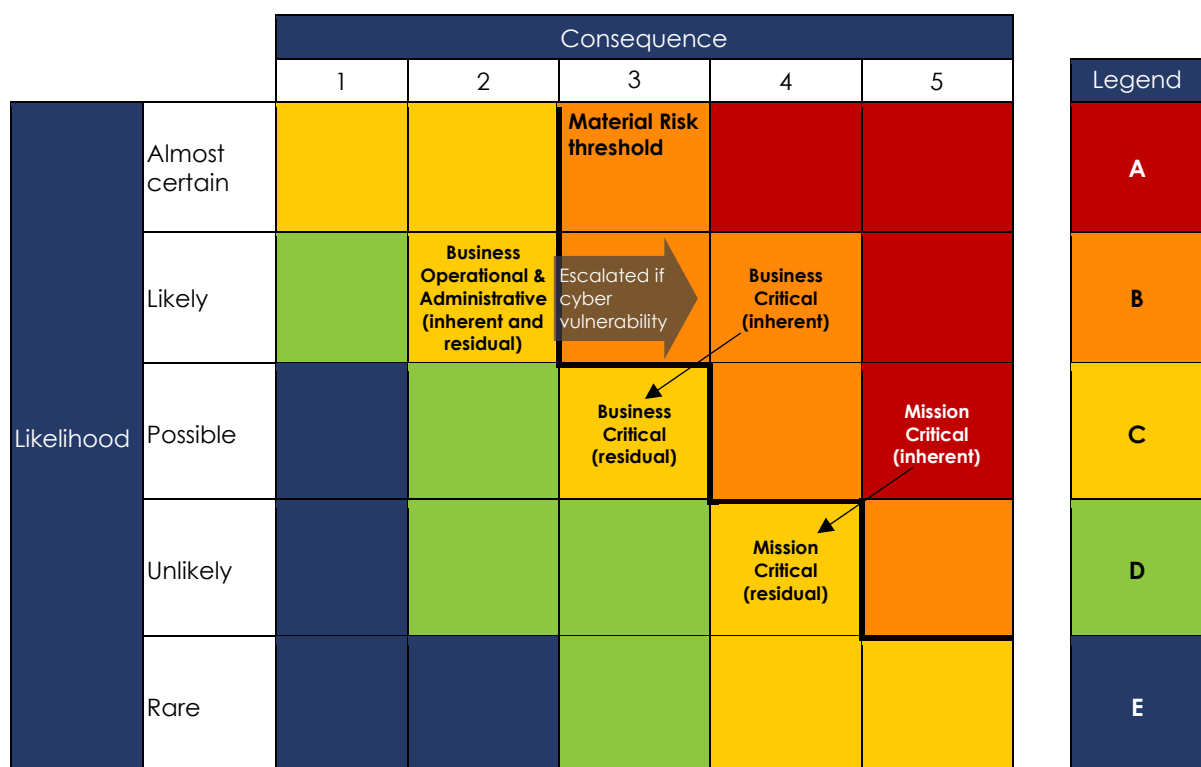
AusNet's preferred lifecycle approach is to replace assets just before the end of extended support, maintaining cost-effective resilience and alignment with industry best practice.

- Mission Critical and Business Critical systems are proactively refreshed to manage residual risk below AusNet's material risk threshold.
- Business Operational and Administrative systems are reactively managed, with upgrades triggered by performance issues or cyber vulnerabilities.

Figure 1 illustrates how this life cycle strategy aligns to our Enterprise Risk Framework. It shows how inherent risk (without mitigations) and residual risk (with implementation of the preferred lifecycle strategy) are assessed relative to AusNet's material risk threshold, with risk levels ranging from red (highest concern) to blue (lowest concern).

This assessment shows that the preferred lifecycle strategy appropriately manages resilience risks; providing a balanced, risk-informed strategy that maintains resilience, optimises cost efficiency, and supports the secure and reliable operation of our electricity distribution network.

Figure 1 – Risk assessment of Mission Critical, Business Critical and Business Operational & Administrative infrastructure



Inherent Risk Ratings

	RISK	CONSEQUENCE	LIKELIHOOD	RISK RATING
Mission Critical	Ageing technology and lack of vendor support to restore services, compounded by limited availability of replacement parts and loss of required skillsets, increasing infrastructure failure, outages, and downtime, causing delays, inefficiencies, and inability to operate and meet customers' expectations.	Level 5. Inoperable Mission Critical systems impact the ability to detect and respond to potential failures and station black events. This could result in widespread power outages and significant NEM disruption, resulting in regulatory and legal consequences, and major reputational damage.	Possible	A

Business Critical	Business wide disruption including inoperable business platforms, unauthorised use of private customer data, inability to undertake financial transactions and make contractual payments, failure to comply with enforceable compliance obligations, fines, and significant reputational harm.	Level 4. Business systems become inoperable causing significant risk of security intrusion, inability to comply with obligations, and financial systems become at risk causing transactions to be delayed. Inoperable systems risk regulatory and legal consequences, reputational damage and major impacts to customer service.	Likely	B
Business Operational & Administrative	Specific business function is unable to be undertaken leading to lower performance, delay in meeting timing, or inefficiency/higher costs.	Level 2. Some business functions may be delayed leading to inefficiencies.	Likely	C

Higher risk where cyber vulnerability identified

2.2. System criticality and revalidation of upgrade timing drivers

For our Revised Proposal, AusNet has applied our enhanced criticality and risk management framework to all our applications and systems. This criticality assessment enables prudent, risk-aware, upgrade deferrals, particularly for the lower criticality Business Operational and Administrative applications.

In addition, to further test the prudence of the program, and in response to the AER's Draft Decision feedback, we have revalidated with infrastructure OEMs and our service management partners the drivers and required timing for proposed upgrades. This revalidation encompasses vendor end of support notifications and upgrade recommendations, where communicated, benchmarking based on the timing of most recent upgrade.

Table 6 details the assessed criticality of each infrastructure component, along with the revalidated upgrade timing driver and rationale.

Table 6 – Infrastructure systems, components and anticipated upgrade drivers, by criticality

Infrastructure system	Description of components	Upgrade drivers
Mission critical infrastructure		
Advanced Distribution Management System (ADMS)	AusNet's network operations and control systems, which provides real-time visibility and control (eg: SCADA), balances supply and demand, and calculates real-time network states based on telemetry and system models.	(C-I-C). Further, the refresh allows AusNet to expand capability in line with planned additions to current ADMS functionality e.g. storm module, historical viewer.
Telecommunications Systems	AusNet utilises telecommunication systems which support SCADA to communicate network state and performance of assets and to respond to emergencies. Includes backup field communication.	(C-I-C).
Data centre facilities	Encompasses critical data centre infrastructure including computer room air-conditioning (CRAC) units and uninterrupted power system (UPS)	AusNet Data Centres house mission-critical IT/OT systems; thus, environmental control (cooling systems) and uninterruptible power supply (UPS) must be assured. (C-I-C). (C-I-C).
Business critical infrastructure		
Distributed Energy Resource Management System (DERMS)	AusNet utilises a platform to manage our customers' rooftop solar to manage supply and demand issues that may have an adverse impact on the security of services. Currently the	DERMS is growing in importance as more DER units connect. The system's hardware must handle increasing data volumes from PV, batteries, EVs, etc.

system is utilised to provide a Victorian Emergency Backstop when rooftop export levels impact the security of the network. The system will also be utilised for flexible exports and forecasting DER penetration and associated constraints on our network. (C-I-C).

System Integration Platforms	Infrastructure that supports the Enterprise Application Integration platforms including (C-I-C).	The integration platform's hardware supports many business systems and is therefore considered business critical. (C-I-C). A hardware failure could cascade into multiple application outages. By keeping the hardware current, AusNet can uphold the resiliency of a critical cross-domain system.
SCADA Data Historian	The infrastructure and storage required to operate the (C-I-C). (SCADA Data Historian).	(C-I-C).
Shared Data Centre Infrastructure	Storage, servers and other computing equipment at each of AusNet's 2 data centres	Shared infrastructure supports multiple critical applications (including some OT systems), so maintaining its reliability is crucial. (C-I-C). Refreshing on schedule ensures continued performance, compatibility with modern software, and support for mission critical services, as older servers may not run new hypervisor versions or security features.
High Security Network (HiSec)	Telecommunications and IT network infrastructure that supports communication to depots and substations for non-SCADA operations.	The HiSec WAN is foundational for both the distribution and transmission operations (shared network for protection telecommunication, SCADA backhaul, etc.). (C-I-C).
Physical Security Digital Infrastructure	Server, network and storage infrastructure required to run security cameras and building access control systems etc. Support the high speed and volume required for the security video footage collected.	Upgrading the CCTV infrastructure is justified by the need for modern surveillance, which includes higher resolution footage, and longer retention to meet security policies. (C-I-C).

Business Operational & Administrative

Data and Analytics	Infrastructure that underpins AusNet's distribution network data and analytics systems, including SNET and Compass.	(C-I-C).
End User Devices	Encompasses laptops, workstations, mobiles and other end user devices.	Extended break fix approaches will be applied to these assets.

2.3. Upgrade costs and Distribution allocations

Cost estimates have been updated as per **Table 7** to reflect the revalidated program and application of our enhanced risk management framework. Updated estimates leverage our infrastructure managed services partner Wipro's domain expertise, alongside AusNet internal costs and historical benchmarks. Wipro is best positioned as AusNet's long-term partner for managing all of our digital and technology infrastructure.

All costs are presented in real 2024 dollars and include AusNet internal program management and architecture costs. Allocation to the distribution network has been applied in accordance with AusNet's Cost Allocation Methodology (CAM) and is detailed for transparency.

Table 7 – System, function and anticipated upgrade timing, by criticality

System or application	Cost estimate basis	Full cost estimate (\$m, real 2024)	Distribution allocation	Distribution cost (\$m, real 2024)
-----------------------	---------------------	-------------------------------------	-------------------------	------------------------------------

Mission critical systems				
Advanced Distribution Management System (ADMS)	Wipro – Cost estimate informed by domain expertise, validated by internal benchmarks, including prior AusNet SCADA/ADMS IT infrastructure purchases.	(C-I-C).	100%	(C-I-C).
Telecommunications Systems	Benchmarked against delivery of comparable initiatives in the current EDPR period.	(C-I-C).	13%	(C-I-C).
Data centre facilities	Wipro – Cost estimate informed by domain expertise, validated by delivery benchmarks from comparable Data Centre Facility upgrades.	(C-I-C).	35%	(C-I-C).
Business critical systems				
Distributed Energy Resource Management System (DERMS)	Wipro – Cost estimate informed by domain expertise, validated by delivery benchmarks from comparable physical server hardware upgrades.	(C-I-C).	100%	(C-I-C).
System Integration Platforms	Wipro – Cost estimate informed by domain expertise, validated by delivery of a similar initiative, where AusNet expanded its integration environment in 2020.	(C-I-C).	49%	(C-I-C).
SCADA Data Historian	Wipro – Cost estimate informed by domain expertise, validated by ongoing replacement costs of OT devices, continuing into the upcoming EDPR period.	(C-I-C).	100%	(C-I-C).
Shared Data Centre Infrastructure	Wipro – Cost estimate informed by domain expertise, validated by delivery benchmarks from comparable data centre infrastructure upgrades.	(C-I-C).	49%	(C-I-C).
High Security Network (HiSec)	AusNet – Cost estimate informed by historical benchmarks and delivery of comparable initiatives in the current EDPR period.	(C-I-C).	23%	(C-I-C).
Physical Security Digital Infrastructure	Wipro – Cost estimate informed by domain expertise, validated by delivery benchmarks from comparable physical security digital infrastructure upgrades.	(C-I-C).	33%	(C-I-C).
Business Operational & Administrative				
Data and Analytics	Benchmarked against delivery of previous upgrades / implementations, (C-I-C).			
	Anticipated scope and capex for these replacements have been reduced in accordance with the Enhanced Systems Criticality and Risk Management framework, given lower system criticality.	(C-I-C).	100%	(C-I-C).
End User Devices	AusNet – Cost estimate informed by historical benchmarks and delivery of comparable initiatives in the current EDPR period.	(C-I-C).	100%	(C-I-C).
	Anticipated scope and capex for these replacements have been reduced in accordance with the Enhanced Systems Criticality and			

Risk Management framework, given
lower system criticality.

3. Evaluation of Options

Based on the infrastructure criticality assessment, and revalidation of required timing and costs, we used risk-cost analysis to determine the optimal strategy for our Revised Proposal expenditure as set out in **Table 8**. We analysed three options that represent differentiation as to whether to proactively refresh infrastructure or reactively manage the risks of not performing lifecycle refreshes.

Table 8 – Options evaluated for Technology Asset Management Infrastructure Revised Proposal

OPTION	SUMMARY
Option 1: Proactive lifecycle refresh on Mission Critical infrastructure only, leveraging vendor extended support arrangement and patch/parts availability.	Ensure that all mission critical infrastructure are refreshed in line with extended support timelines and/or expected extended life of infrastructure. However, run business-critical and business operations and administration infrastructure without performing lifecycle refreshes, reactively managing the consequences in-house.
Option 2: Proactive lifecycle refresh on Mission and Business Critical infrastructure, leveraging vendor extended support arrangement and patch/parts availability.	Ensure that all mission-critical and business-critical infrastructure are refreshed in line with extended support timelines and/or expected extended life of infrastructure. However, reactively manage business operations and administration infrastructure.
Option 3: Proactive lifecycle refresh of all infrastructure and maintain with vendor mainstream support.	Ensure that all infrastructure are refreshed in line with mainstream support timelines and/or expected standard life of infrastructure.

3.1. Option 1 – Proactive refreshes on Mission Critical infrastructure only

Under this option, we would perform lifecycle refreshes and upgrades in line with vendor extended support agreements (i.e. in line with vendor end of extended support dates), only on Mission Critical infrastructure including data centre facilities, telecommunications, and ADMS hardware. This reflects the criticality of this infrastructure to supporting mission critical applications that maintain distribution network operations. Under this option, Business Critical and Business Operational & Administrative infrastructure would be reactively managed with limited or no vendor support in a run to failure mode.

Risk assessment of this option is shown in **Table 9** below, which shows reduction in network outage risk – our control systems (e.g. SCADA) are less likely to become inoperable and response time improved. Other risk levels remain unchanged from inherent levels, with business wide disruption risk remaining above AusNet's material risk threshold.

Table 912 - Risk assessment of Option 1

		Consequence				
		1	2	3	4	5
Likelihood	Almost certain			Material Risk threshold		
	Likely		R1.3		R1.2	
	Possible					
	Unlikely				R1.1	
	Rare					

Legend

A

B

C

D

E

RISK	CONSEQUENCE	LIKELIHOOD	RISK RATING
R1.1	Increases system failures, outages and downtime causing delays, inefficiencies and inability to operate and meet customers' expectations from the business	Unlikely	C

		response to the event, leading to less outage time.		
R1.2	Business wide disruption including inoperable business platforms, unauthorised use of private customer data, inability to undertake financial transactions and make contractual payments, failure to comply with enforceable compliance obligations, fines, and significant reputational harm.	Level 4. Business systems become inoperable causing significant risk of security intrusion, inability to comply with obligations, and financial systems become at risk causing transactions to be delayed.	Possible	B
R1.3	Specific business function is unable to be undertaken leading to lower performance, delay in meeting timing, or inefficiency/higher costs.	Level 2 – Some business functions may be delayed leading to inefficiencies.	Likely	C

Table 10 below shows the costs of this option. Reactive management of Business Critical and Business Operational & Administrative infrastructure in-house is anticipated to require higher opex due to growth in the support organisation required to provide response to issues and outages.

Table 103 4- Forecast expenditure for Option 1 (\$million real 2024, distribution network allocated costs)

Cost item	RY27	RY28	RY29	RY30	RY31	Total
Capex	2.9	2.5	2.6	4.8	5.2	18.0
Opex	1.5	1.0	0.8	0.4	0.4	4.2
Total	5.8	3.0	4.8	9.5	6.1	22.2

3.2. Option 2 – Proactive refreshes on Mission and Business Critical infrastructure only

This option seeks to perform lifecycle refreshes and upgrades in line with vendor extended support agreements (i.e. in line with vendor end of extended support dates) on both Mission Critical and Business Critical infrastructure. We would reactively manage infrastructure categorised as Business Operational & Administrative such as user devices with limited or no vendor support.

As can be seen from **Table 11**, this option manages all risks to below AusNet's Material Risk threshold. This is achieved by addressing the distribution network operations and business disruption risks posed by resilience or cyber vulnerabilities to Mission and Business Critical infrastructure. Business efficiency risks remain unchanged from inherent ratings, with ongoing reactive management.

Table 115 - Risk assessment of Option 2

		Consequence					Legend
		1	2	3	4	5	
Likelihood	Almost certain			Material Risk threshold			
	Likely		R2.3				
	Possible			R2.2			
	Unlikely				R2.1		
	Rare						
							A
							B
							C
							D
							E

	RISK	CONSEQUENCE	LIKELIHOOD	RISK RATING
R2.1	Increases system failures, outages and downtime causing delays, inefficiencies and inability to operate and meet customers' expectations from the business	Level 4. Significant consequence if outage occurs but capability for the business to respond quicker given that mission critical systems are operable in response to the event, leading to less outage time.	Unlikely	C
R2.2	Business wide disruption including inoperable business platforms, unauthorised use of private customer data, inability to undertake financial transactions and make contractual payments, failure to comply with enforceable compliance obligations, fines, and significant reputational harm.	Level 4. Reduced impact of security intrusion, with reduced vulnerability and greater data security across breadth of applications, plus vendor support to manage detection and response.	Possible	C
R2.3	Specific business function is unable to be undertaken leading to lower performance, delay in meeting timing, or inefficiency/higher costs.	Level 2 – Some business functions may be delayed leading to inefficiencies.	Possible	C

Table 12 below shows the costs of this option. Capex is higher than Option 1 to the refreshes for Business Critical system but incremental opex is not required. While the cost of this option is higher than Options 1 the risks of both energy network and business-wide disruption have significantly reduced.

Table 12 - Forecast expenditure for Option 2 (\$million real 2024, distribution network allocated costs)

Cost item	RY27	RY28	RY29	RY30	RY31	Total
Capex	5.1	4.0	4.7	5.7	6.1	25.6
Opex	-	-	-	-	-	-
Total	5.1	4.0	4.7	5.7	6.1	25.6

3.3. Option 3 – Proactive lifecycle refreshes for all infrastructure

This option involves implementing a lifecycle refresh across all infrastructure assets in line with vendor's end of mainstream support. Mainstream supports provides some added confidence that all infrastructure will have readily available spares and patches. Duration of incidents will marginally reduce as vendors will have sufficient spares and replacements on hand. Triggering replacement at end of mainstream support rather than end of extended support will result in the earlier replacement of assets when compared to Option 2, which is reflected in incremental cost for Option 3. Risk reduction will be realised for Business Operation and Administrative systems which will move from reactive to proactive management.

This option reduces to the risk to as low as reasonably practical; minimising likelihood and consequences relative to Options 1 and 2. This can be seen in **Table 13** where there is lower risk of incidents resulting in in disruption or inefficiency of specific business activities.

Table 13 - Risk assessment of Option 3

		Consequence					Legend
		1	2	3	4	5	
Likelihood	Almost certain			Material Risk threshold			
	Likely						
	Possible		R3.3	R3.2			
	Unlikely				R3.1		
	Rare						
							A
							B
							C
							D
							E

	RISK	CONSEQUENCE	LIKELIHOOD	RISK RATING
R3.1	Increases system failures, outages and downtime causing delays, inefficiencies and inability to operate and meet customers' expectations from the business	Level 4. Reduced impact of outages that limit end users from conducting their business as usual and slows down the business' ability to respond to operational incidents both internally and externally. Impact reduced as more limited potential for cascading dependency outages, and more timely response with vendor support	Unlikely	C
R3.2	Business wide disruption including inoperable business platforms, unauthorised use of private customer data, inability to undertake financial transactions and make contractual payments, failure to comply with enforceable compliance obligations, fines, and significant reputational harm.	Level 4. Reduced impact of security intrusion, with reduced vulnerability and greater data security across breadth of applications, plus vendor support to manage detection and response	Unlikely	C
R3.3	Specific business function is unable to be undertaken leading to lower performance, delay in meeting timing, or inefficiency/higher costs.	Level 3. Reduced impact with reporting unlikely to be delayed but will require a greater amount of effort	Unlikely	D

Table 14 below shows the costs of this option. Capex is higher than Option 1 and 2 as earlier and proactive refreshes are required for all infrastructure.

Table 14 - Forecast expenditure for Option 3 (\$million real 2024, distribution network allocated costs)

Cost item	RY27	RY28	RY29	RY30	RY31	Total
Capex	7.8	6.3	6.6	8.0	10.3	39.0
Opex	-	-	-	-	-	-
Total	7.8	6.3	6.6	8.0	10.3	39.0

3.4. Recommended option

Based on the assessment of options, proactive refreshes for Mission Critical and Business Critical applications and systems (Option 2), is the recommended option. This option most cost effectively manages digital resilience risks within AusNet's Material Risk threshold.

The cost of this recommended option is \$25.6m capex (\$real 2024), which represents a \$4.0m capex reduction relative to AusNet's initial proposal. The summary of this assessment is detailed in **Table 14** below.

Table 14 Evaluation of TAM Applications expenditure options (\$m real 2024, distribution network allocated costs)

Criteria	Option 1	Option 2	Option 3	Initial Proposal
Capex (\$million, real 2024)	22.2	25.6	39.0	29.6
Opex (\$million, real 2024)	4.2	-	-	-
Reduces risks below Material Risk threshold	✗	✓	✓	✓
Preferred option	✗	✓	✗	✗

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

