

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

### Resubmission Addendum: Technology Asset Management - Applications

Date: 1 December 2025



# Table of contents

<b>Executive Summary</b>	<b>4</b>
<b>1. AusNet's proposal and AER Draft Decision</b>	<b>6</b>
1.1. Initial Submission Summary	6
1.2. AER Draft Decision feedback	6
<b>2. AusNet's Revised Proposal</b>	<b>8</b>
2.1. Enhanced approach to managing digital resilience risks	8
2.2. System criticality and revalidation of upgrade timing drivers	9
2.3. Upgrade costs and Distribution network allocations	12
2.4. Review for synergies	14
<b>3. Evaluation of Options</b>	<b>15</b>
3.1. Option 1 – Proactive refreshes on Mission Critical systems only	15
3.2. Option 2 – Proactive refreshes on Mission and Business Critical systems only	16
3.3. Option 3 – Proactive lifecycle refreshes for all systems	17
3.4. Recommended option	18

## Document history

DATE	VERSION	COMMENT
10/11/2025	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

The Technology Asset Management (TAM) Applications program is AusNet's recurrent expenditure to maintain the resilience and existing capabilities of the technology applications that enable us to deliver an affordable and reliable distribution network service to our customers. Through this program AusNet applies a risk-based lifecycle refresh approach to maintain application currency and supportability, consistent with our risk management policies.

The AER's Draft Decision did not approve AusNet's initial proposal for TAM Applications. The AER Draft Decision included alternative capex and opex forecasts as detailed in **Table 1** below.

**Table 1 - AusNet Initial Proposal and AER Alternative Forecast (\$m, real FY2026)**

Cost item	AusNet Initial Proposal	AER Alternative	Adjustment
Capex	\$67.3M	\$41.3M	-39%
Opex	\$3.9M	\$1.3M	-67%

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

AER Draft Decision Feedback	How this has been addressed in AusNet's Revised Proposal
Not considering a strategy of prioritising which applications to upgrade and seeking opportunities for prudent risk-aware deferrals (extensions to lifecycles)	<ul style="list-style-type: none"> <li>AusNet has recently implemented an enhanced systems criticality and risk management framework, which has been applied for the Revised Proposal, guiding our approach to both proactive and reactive refreshes.</li> <li>The application of this framework has reduced forecast refresh requirements for lowest criticality Business Operational &amp; Administrative applications.</li> <li>Detailed consultation with (C-I-C) has enabled deferral of planned ADMS (C-I-C), replacing it with a lower cost version upgrade.</li> <li>AusNet is preparing for its first DERMS upgrade, which has now informed the scope and timing of upgrades planned during the regulatory period.</li> </ul>
Cost estimates not based on referenceable bottom-up assessments, with potential for over-estimation bias	<ul style="list-style-type: none"> <li>AusNet has revalidated cost estimates, incorporating updated project figures since the initial submission (ADMS and GE Smallworld upgrades) to refine our revised proposal against historical benchmarks.</li> <li>Where there were no historical benchmarks available, our digital implementation partner (Wipro) has completed cost estimates.</li> </ul>
Requirement to review TAM program scope relative to non-recurrent programs, to identify any cost efficiency synergies	<ul style="list-style-type: none"> <li>Cost efficiencies have been included in the submission e.g. SCADA upgrade was excluded from TAM as non-recurrent ADMS program makes this unnecessary.</li> <li>Within the program, initiatives have been optimised to leverage synergies e.g. ERP (C-I-C) and Energy Data Management (C-I-C) will be executed in parallel to optimise cost, similarly ADMS and (C-I-C) upgrades will be executed in parallel to optimise cost.</li> </ul>
Allocation of project costs between AusNet's distribution, transmission and gas network businesses	<ul style="list-style-type: none"> <li>AusNet's initial proposal reflected only distribution network allocated costs, in line with our Cost Allocation Methodology (CAM). In our revised proposal, shared system allocations have been clearly documented, with distribution network allocated costs, as per our Cost Allocation Methodology.</li> </ul>
Opex step change: "forced" cloud migrations may require some additional opex, however lower, and insufficient ADMS Calltaker step change justification	<ul style="list-style-type: none"> <li>(C-I-C) has informed AusNet that new licenses will be required for the ADMS Call Taker (C-I-C) due to a change in the licensing model. The opex reflects the (C-I-C) license costs.</li> </ul>

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 application criticality categories. The results of this assessment are details in **Table 2**, with the preferred Option 2 providing optimum 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 systems only	\$37.2M	No	No
2	Proactive refreshes on Mission and Business Critical systems only	\$47.7M	Yes	<b>Yes</b>
3	Proactive lifecycle refreshes for all systems	\$53.3M	Yes	No

Based on this assessment, AusNet's Technology Asset Management – Applications revised proposal represents \$45.7m capex and \$2.0m opex. All costs represent distribution network allocation. Expenditure profile through the FY2027-31 regulatory period is detailed in **Table 3** below.

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

Cost item	FY2027	FY2028	FY2029	FY2030	FY2031	Total
<b>Capex</b>	\$8.9M	\$7.7M	\$9.9M	\$8.5M	\$10.7M	<b>\$45.7M</b>
<b>Opex</b>	\$0.7M	\$0.0M	\$0.3M	\$0.5M	\$0.5M	<b>\$2.0M</b>
<b>Total</b>	<b>\$9.6M</b>	<b>\$7.7M</b>	<b>\$10.2M</b>	<b>\$9.0M</b>	<b>\$11.2M</b>	<b>\$47.7M</b>

# 1. AusNet's proposal and AER Draft Decision

AusNet has over 200 technology systems and applications that help us deliver an affordable and reliable distribution network service to our customers. They support key functions such as operating our network safely and reliably, providing customers with information on outages and enabling communications, ensuring network bills are accurate, assisting efficient asset planning, and ensuring our business is run efficiently.

This section summarises AusNet's initial FY2027-31 regulatory period proposal for "Technology Asset Management" (TAM): recurrent expenditure to maintain the resilience and existing capabilities from those technology applications that underpin our distribution network service. 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 revised proposal.

## 1.1. Initial Submission Summary

AusNet's initial submission proposed expenditure to maintain currency and supportability of our systems and applications, consistent with our ICT and risk management policies. Upgrade needs in the FY2027-31 period were identified through a bottom-up assessment of each of our applications and systems to determine the known or likely timing of vendor updates, patches and bug fixes. Cost estimates were developed based on historical benchmarks for similar upgrades and through workshop engagement with AusNet's digital partners and represented the distribution network's cost allocations where systems are shared across AusNet's regulated networks.

Based on assessment of the risk and cost of varying options, including actively managing without vendor support or upgrading only critical operational systems, AusNet proposed expenditure of \$60.8m capex and \$3.7m opex (\$real 2024) for application lifecycle refreshes, as shown in **Table 4** below. Opex expenditure in this forecast represented anticipated incremental licencing costs for forced migrations to cloud solutions, recognising the trend for some vendors to move new application versions solely to the cloud, and incremental licencing and support costs for the new ADMS Calltaker application version (as advised by C-I-C).

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

Cost item	FY27	FY28	FY29	FY30	FY31	Total
Capex	\$7.6M	\$9.6M	\$16.11M	\$13.6M	\$14.0M	<b>\$60.8M</b>
Opex	\$0.5M	\$0.8M	\$0.8M	\$0.8M	\$0.8M	<b>\$3.7M</b>
Total	<b>\$8.1M</b>	<b>\$10.4M</b>	<b>\$16.9M</b>	<b>\$14.4M</b>	<b>\$14.8M</b>	<b>\$64.5M</b>

## 1.2. AER Draft Decision feedback

The AER did not accept AusNet's proposed expenditure and the Draft Decision included an alternative forecast of \$41.3m capex and \$1.3m opex (\$real 2026), per **Table 5** below.

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

Cost item	Initial Proposal	AER Alternative	Adjustment
Capex	\$67.3M	\$41.3M	-39%
Opex	\$3.9M	\$1.3M	-67%

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

- Not considering a strategy of prioritising which applications to upgrade and seeking opportunities for prudent risk-aware deferrals (extensions to lifecycles)
- Requirement to review TAM program scope relative to non-recurrent ICT programs, to identify any synergies that may result in cost efficiencies
- Cost estimates not based on referenceable bottom-up assessments, with potential for over-estimation bias. EMCa specifically highlight ERP, ADMS, DERMS and other business systems upgrade costs
- Allocation of project costs between AusNet's distribution, transmission and gas network businesses

The AER Draft Decision accepted the forced cloud migrations component of proposed opex step change, with adjustment applied for allocation of project costs between AusNet's lines of business (initial proposal \$2.7m reduced to \$1.3m in AER Alternative forecast).

The AER and EMCa provided two specific items of feedback on the proposed opex step change:

- EMCa concluded that some additional opex for "forced" migrations to the cloud may be required, however due to cost allocation this would be less than proposed
- Insufficient supporting justification was provided for the ADMS Calltaker proposed step change

## 2. AusNet's Revised Proposal

In response to the AER's Draft Decision, AusNet has reviewed the Technology Asset Management – Applications 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 risks

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

Through 2025 we have implemented an enhanced criticality assessment and risk management framework to manage the resilience risks of our applications and systems. This enhanced framework sees applications and systems classified into three criticality categories, which underpin our assessment of the risks they pose in terms of resilience and cyber security. These categories guide our approach of either proactively updating when vendors provide notice of upgrades or patches, or pursuing prudent deferrals and reactively undertaking updates on systems when vulnerabilities or functional failures are identified. Implementation of this criticality assessment and risk management framework is consistent with the AER Draft Decision feedback of prioritising applications for upgrade and seeking opportunities for prudent risk-aware deferrals.

The three criticality categories, and AusNet's risk management approach for each, are detailed below:

- **Mission Critical** (proactive management) – These are applications and systems that are essential to providing electricity to our customers as defined by the risk of a widescale and extended power outage. A key example of a risk to a Mission Critical system is the inoperability of SCADA leading to loss of electricity network control. Given the criticality of these systems, our approach is to proactively update systems and undertake patching in accordance with vendor updates to reduce risks as far as reasonably practical.
- **Business Critical** (proactive management) – These are systems that would cause significant business disruption, resulting in regulatory compliance exposures, reputational risks, and significant increases in costs. A key example of a Business Critical system is the Enterprise Resource Planning (ERP) system which is central to asset management, finance and compliance. Consistent with mission critical systems, given the risks that outages to Business Critical systems pose, our approach is to proactively update and undertake patching in accordance with vendor recommendations.
- **Business Operational and Administrative** (reactive management) – These are systems that while important for ongoing business function and efficiency, they are not directly related to the energy network operability, as an outage would not create widescale business disruption. Our approach for these systems is to reactively manage (and prudently defer where appropriate) the vendor recommended upgrades and patching. Under this approach we actively manage cost vs risk trade-offs, and progress upgrades when functionality is impacted or when cyber vulnerabilities are identified. This approach can result in delayed upgrade cycles relative to vendor recommendations, with resilience or functionality impacts actively managed. However, identified cyber security vulnerabilities will be remediated, given the cyber intrusion risk that any single application or system can pose (the “weakest link”). In effect, remediation of cyber security vulnerabilities can become the driver for upgrades of this classification of systems and applications.

**Figure 1** articulates our criticality assessment and risk management framework, relative to AusNet's Enterprise Risk Management Framework. Risks of highest concern are rated red, those of lowest concern are rated blue, and AusNet's Material Risk threshold is shown. Inherent risk represents assessment in the absence of prescribed risk mitigations, with residual risk representing assessment with these mitigations in place (i.e. upgrades and patching).

Mission Critical and Business Critical systems pose inherent risks above our material risk threshold. Implementing version updates, patches and bug fixes moves the residual risk to tolerable risk levels. The inherent risk posed by Business Operational and Administrative systems is lower, and hence the more cost-effective reactive risk management approach is acceptable; noting that a reactive approach still requires responding to events, and updating systems when a risk of failure has been detected. Where a cyber security vulnerability is specifically identified this inherent risk escalates and will drive an upgrade if required to mitigate the cyber risk.



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

		Consequence					Legend
		1	2	3	4	5	
Likelihood	Almost certain			Material Risk threshold			A
	Likely		Business Operational & Administrative (inherent and residual)	Escalated if cyber vulnerability	Business Critical (inherent)		B
	Possible			Business Critical (residual)		Mission Critical (inherent)	C
	Unlikely				Mission Critical (residual)		D
	Rare						E

#### Inherent Risk Ratings

	RISK	CONSEQUENCE	LIKELIHOOD	RISK RATING
<b>Mission Critical</b>	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, leading to regulatory and legal consequences, and major reputational damage.	Possible	A
<b>Business Critical</b>	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
<b>Business Operational &amp; Administrative</b>	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 application vendors, and our implementation partners the 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 system and application, along with the revalidated upgrade timing driver and rationale. Key outcomes from this review, resulting in updates to AusNet's Revised Proposal are:

- Data and Analytics, Health Safety Environment & Quality, and Other Operational Business Systems assessed as lowest criticality Business Operational & Administrative systems, presenting opportunity to prudently extend lifecycles and reduce required expenditure
- In consultation with (C-I-C) following their 2025 roadmap update, (C-I-C) have confirmed there will be ongoing support for AusNet's current ADMS platform through FY2031. AusNet's initial proposal had planned migration to (C-I-C) platform, which has now been deferred and replaced with a reduced cost and complexity ADMS upgrade. (C-I-C) have advised that (C-I-C) migration will be prioritised for AusNet's transmission platform (C-I-C) with the (C-I-C) ADMS Calltaker being the first distribution ADMS module available in 2027/2028.

**Table 6 – System, function and anticipated upgrade timing, by criticality**

System or application [Vendor Product]	Description of function	Upgrade timing drivers
<b>Mission critical systems</b>		
Advanced Distribution Management System (ADMS) (C-I-C)	AusNet's network operations and control systems, which provide real-time visibility and control (e.g. SCADA), balances supply and demand, and calculates real-time network states based on telemetry and system models.	(C-I-C)
ADMS Calltaker (C-I-C)	Calltaker is used by the customer contact centre to raise and query customer fault calls. These calls are used by ADMS to infer network outages generating trouble calls.	Currently the ADMS (C-I-C) provide a rudimentary Calltaker capability. (C-I-C) intends to deprecate this capability and replace it with a more function standalone ADMS Calltaker based on their new (C-I-C)  In line with the ADMS upgrade (described above) AusNet will implement the new (C-I-C) ADMS Calltaker. This will be undertaken in 2030/2031 to ensure the product is mature before AusNet adopts it, providing a low risk first transition for the (C-I-C) architecture in the ADMS suite.
Telecommunications Systems (C-I-C)	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). AusNet reasonably expects to upgrade these systems in the coming regulatory period.
Identity Management (C-I-C)	For security purposes, AusNet has a system that enables core identity and access to systems, with multiple instances to maintain OT/IT separation. The system provides functions such as single sign on and two factor authentication for employees and contractors which require access to AusNet systems.	(C-I-C). These domain servers will need to be upgraded during the coming regulatory period.

## Business critical systems

Enterprise Resource Planning (ERP) (C-I-C)	AusNet uses an ERP to manage business transactions and data across functions in a single integrated system. This includes finance, human resources, procurement, asset and works management.	(C-I-C), to ensure that AusNet maintains vendor support and receives critical patches.
Distributed Energy Resource Management System (DERMS) (C-I-C)	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 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.	DERMS was first implemented as part of the Solar Emergency Backstop project in 2024 in line with AusNet's work to accommodate a rapidly evolving DER market.  As the DERMS product is a relatively new product which is going through significant evolutions to support scalability and performance, AusNet will be required to upgrade (C-I-C) DERMS within the regulatory period.
Customer Systems (C-I-C)	Through our website, AusNet provides information to our customers and community including outage tracking. Our customer portals enable customers to connect to our network, make claims and report faults.	(C-I-C)
Geospatial Systems (C-I-C)	AusNet uses Geographic Information Systems (GIS) to manage an accurate, comprehensive and integrated geospatial view of the entire network including its characteristics to assist with asset management planning and design	(C-I-C)
System Integration Platforms (C-I-C)	AusNet uses a cohesive set of integration software (middleware) products that enable data exchange and processes between applications. This includes an Application Programming Interface (API) that provides protocols for software applications to communicate with each other. We also use data integration to combine and harmonise data from into a unified, format for analysis.	(C-I-C)
Network Billing (C-I-C)	AusNet uses a network billing system to meet its obligations to bill a customer's retailer based on approved network tariffs and energy usage and those services we contract for directly.	(C-I-C). AusNet would expect to upgrade the system in the coming regulatory period.
SCADA Data Historian (C-I-C)	AusNet utilises SCADA to monitor and control assets on the high and medium voltage sections of its network. The historian is a vital element of the SCADA system that logs and stores data over time and enables us to carry out time-series analysis on network performance.	(C-I-C)
Weather and Solar Services (C-I-C)	Ausnet uses applications that provides solar irradiance and weather data from data providers which are integrated into various systems to ensure the reliability and	(C-I-C) services which are integrated into various systems and process. As a result, these require a more continuous change cycle as the vendors replaces and depreciate APIs or features.

	security of the distribution network and for forecasting purposes	
Protection and Control Settings (C-I-C)	AusNet uses power system modelling software for secondary protection settings and DFA schemes	(C-I-C). Based on this IT cycle, AusNet expects at least one upgrade in the coming regulatory period.
Network Access Management (C-I-C)	AusNet uses systems that request and authorise access to the network to perform maintenance tasks.	(C-I-C) Ausnet plans to expand/enhance this platform in 2029 under the ADMS program. As a result, this recurrent investment has been deferred to 2031 to reflect continued maintenance that is required to upgrade external libraries, DB, operating system, etc. (C-I-C)

#### Business Operational & Administrative

Data and Analytics (C-I-C)	AusNet uses a combination of on-premise and on-cloud enterprise data analytics and warehouse solutions which aggregates data from many different sources into a central and consistent data repository to support data analysis and reporting.	The capex costs are primarily driven by the on-premise systems, (C-I-C). AusNet would expect to upgrade these systems in the coming regulatory period. Some continued investment in the (C-I-C) Data & Analytics PaaS platform is expected as (C-I-C) replace and depreciate APIs or features.
Health Safety Environment and Quality (C-I-C)	Ausnet uses systems to track, monitor and report on Health, Safety, Environment and Quality functions including risk management.	This is a collection of systems that require continuous investment driven by new audit requirements, regulatory changes and changing government policies.
Other operational business systems (C-I-C)	For simplicity, AusNet has grouped an array of specific business function applications that require minimal expenditure to update. The applications provide capabilities including engineering and design, Human Resources, contract assessment, and information management.	This is a collection of small business function systems where the investment is driven by risk or need, not by vendor end of life. These systems require small amounts of ongoing investment to meet business/regulatory changes and risks e.g. to address security issues.

## 2.3. Upgrade costs and Distribution network allocations

To address the AER's Draft Decision feedback, AusNet has revalidated cost estimates for each system and application upgrade, incorporating scope revisions as detailed in Section 2.2.

As the majority of planned upgrades are comparable to previously completed projects, AusNet internal costs and historical benchmarks have been used. For specific systems and applications where historical benchmarks are not available, such as the recently implemented DERMS and ERP systems, AusNet's delivery partner Wipro have provided cost estimates. Wipro is best positioned to provide these estimates, having led implementation of the relevant systems, and continuing to manage their ongoing operation, and through leveraging global domain expertise.

Cost estimates are detailed in **Table 7** below. 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)
<b>Mission critical systems</b>				
Advanced Distribution Management System (ADMS)	Benchmarked to comparable upgrade being delivered in 2025/2026. (Noting scope revised to ADMS upgrade vs (C-I-C) migration in initial proposal)	(C-I-C)	100%	(C-I-C)
ADMS Calltaker	Wipro – Costs forecast using domain expertise and delivery benchmarks from comparable programs. Incremental opex licencing costs for new (C-I-C) cost per NMI quotation.	(C-I-C)	100%	(C-I-C)
Telecommunications Systems	Benchmarked against delivery of comparable initiatives in the current EDPR period.	(C-I-C)	100%	(C-I-C)
Identify Management	Costs forecast based on delivery of comparable initiative/s within current EDPR regulatory period.	(C-I-C)	49%	(C-I-C)
<b>Business critical systems</b>				
Enterprise Resource Planning (ERP)	Wipro – Delivered (C-I-C) migration, costs forecast will be based on first upgrade.	(C-I-C)	49%	(C-I-C)
Distributed Energy Resource Management System (DERMS)	Wipro – Costs forecast using domain expertise, noting this is the first proposed DERMS upgrade in the EDPR.	(C-I-C)	100%	(C-I-C)
Customer Systems	Benchmarked against delivery of previous upgrade from (C-I-C).	(C-I-C)	70%	(C-I-C)
Geospatial Systems	Benchmarked against delivery of inflight upgrade to (C-I-C). Benchmarked against delivery of (C-I-C).	(C-I-C)	62%	(C-I-C)
System Integration Platforms	Benchmarked against delivery of previous upgrade to (C-I-C).	(C-I-C)	49%	(C-I-C)
Network Billing	Benchmarked against delivery of previous upgrade in 2023.	(C-I-C)	70%	(C-I-C)
SCADA Data Historian	Benchmarked against delivery of comparable initiatives in the current EDPR period.	(C-I-C)	62%	(C-I-C)
Weather and Solar Services	Benchmarked against delivery of comparable initiatives in the current EDPR period.	(C-I-C)	62%	(C-I-C)
Protection and Control Settings	Benchmarked against delivery of previous upgrades within the current EDPR period.	(C-I-C)	62%	(C-I-C)
<b>Business Operational &amp; Administrative</b>				
Data and Analytics (On Premise)	Benchmarked against delivery of previous upgrades / implementations, (C-I-C).  Capex for this initiative has been reduced in accordance with the enhanced systems criticality	(C-I-C)	100%	(C-I-C)

	and risk management framework, which classified it as low criticality.			
Data and Analytics (Cloud)	Costs forecast based on delivery of comparable initiative/s within current EDPR regulatory period.  Capex for this initiative has been reduced in accordance with the Enhanced Systems Criticality and Risk Management framework, which classified it as low criticality.	(C-I-C)	49%	(C-I-C)
Health, Safety, Environmental and Quality	Costs forecast based on delivery of comparable initiative/s within current EDPR regulatory period.  Capex for this initiative has been reduced in accordance with the Enhanced Systems Criticality and Risk Management framework, which classified it as low criticality.	(C-I-C)	49%	(C-I-C)
Other operational business systems	Costs forecast based on delivery of comparable initiative/s within current EDPR regulatory period.  Capex for this initiative has been reduced in accordance with the Enhanced Systems Criticality and Risk Management framework, which classified it as low criticality.	(C-I-C)	49%	(C-I-C)

## 2.4. Review for synergies

As part of AusNet's initial EDPR Submission, we assessed the recurrent TAM delivery and expenditure against the proposed non-recurrent investment programs delivering new initiatives. Consequently, we identified opportunities to optimise recurrent Capex spend, achieved through a combination of initiative descoping, consolidation and schedule optimisation. This assessment was revalidated for our Revised Proposal, with program optimisations detailed below:

### Recurrent Applications Capex - Optimisations:

- Removed the recurrent SCADA (Distribution) upgrade from the TAM program. The ADMS program's SCADA and eFEPs initiative will replace the existing SCADA therefore it is not necessary to upgrade the existing system.
- Reduced and deferred the recurrent maintenance on the Network Access Management. The ADMS Network Access, Authorisations & Switching initiative will result in new capabilities that will also cover any maintenance requirements in 2029. This will reduce and defer most of the maintenance activities until 2031.
- Concurrently execute Energy Data Management (C-I-C) initiative and Core (C-I-C) upgrade to achieve delivery efficiencies. This approach was used in the 2024 (C-I-C) upgrade successfully and is therefore the assumed approach in the TAM program.
- Concurrently execute the ADMS – Calltaker (C-I-C) alongside ADMS upgrade to achieve inter-project synergies. This removed the need to decommission or recommission the old Calltaker environment which has been superseded by the (C-I-C) version.

## 3. Evaluation of Options

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

**Table 8 – Options evaluated for Technology Asset Management Applications Revised Proposal**

OPTION	SUMMARY
<b>Option 1:</b> Proactive lifecycle refresh on Mission Critical systems only, in-line with vendor recommendations	Proactively maintain Mission Critical systems with most current updates and patching. Reactively manage Business Critical and Business Operational & Administrative systems, without proactive updates or patches and actively managing resilience exposures and cyber vulnerabilities as they present.
<b>Option 2:</b> Proactive lifecycle refresh on Mission and Business Critical systems, in line with vendor recommendations	Proactively maintain Mission Critical and Business Critical systems with current updates and patching. Reactively manage Business Operational & Administrative systems, progressing upgrades on a risk-cost assessment basis when resilience risks and cyber vulnerabilities as they present.
<b>Option 3:</b> Proactive lifecycle refresh and patching on all systems in line with vendor recommendations	Proactively ensure that all applications and systems are refreshed with most current updates and patched, including Mission Critical, Business Critical and Business Operational & Administrative.

### 3.1. Option 1 – Proactive refreshes on Mission Critical systems only

Under this option, we would perform proactive lifecycle refreshes and patches on all Mission Critical systems (e.g. ADMS, identity management and telecommunications systems). This reflects the criticality of these systems to energy network operation and customer supply. Under this option, Business Critical and Business Operational & Administrative systems would be actively reactively managed.

As can be seen from **Table 9** below, this option reduces energy network operations risks – our control systems are less likely to become inoperable, and with vendor support response time to any event is reduced. However, business risks, such as regulatory and financial compliance, remain elevated and above the Material Risk threshold due to reactive management of Business Critical systems.

**Table 9 - Risk assessment of Option 1**

		Consequence					Legend
		1	2	3	4	5	
Likelihood	Almost certain			Material Risk threshold			
	Likely		R2.3		R2.2		
	Possible						
	Unlikely				R2.1		
	Rare						
							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	Level 4. Significant consequence if outage occurs but capability for the business to respond quicker given that mission critical systems are	Unlikely	C



		operable in 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

Higher risk where cyber vulnerability identified

Costs for this option are shown in **Table 10** below. Reactive management of applications in-house, without vendor support, is anticipated to require progressively higher opex due to growth in the support organisation required to provide response to issues and outages, and to retain knowledge of legacy applications. Further capex would still be required for upgrades when an incident demonstrates that an upgrade or patching would prevent future occurrence of the incident.

**Table 10 - Forecast expenditure for Option 1 (\$m real 2024, distribution network allocated costs)**

Cost item	FY27	FY28	FY29	FY30	FY31	Total
Capex	\$4.2M	\$5.0M	\$5.1M	\$7.0M	\$8.8M	\$30.2M
Opex	\$2.1M	\$1.0M	\$1.8M	\$1.0M	\$1.1M	\$7.0M
Total	\$6.3M	\$6.0M	\$6.9M	\$8.0M	\$9.9M	\$37.2M

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

This option seeks to perform lifecycle refreshes and patches on both Mission Critical and Business Critical systems. Business Operational & Administrative systems would be reactively managed, upgrades assessed on a cost vs risk trade-off when functionality is impacted or when cyber vulnerabilities are identified.

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 energy network operations and business disruption risks posed by resilience or cyber vulnerabilities to Mission and Business Critical systems. Business efficiency risks remain unchanged from Section 1.3 inherent risk, with ongoing reactive management (particularly focused on cyber vulnerabilities).

**Table 11 - Risk assessment of Option 2**

		Consequence					Legend
		1	2	3	4	5	
Likelihood	Almost certain			Material Risk threshold			
	Likely		R3.3				
	Possible			R3.2			
	Unlikely				R3.1		
	Rare						

	RISK	CONSEQUENCE	LIKELIHOOD	RISK RATING
R3.1	Increases system failures, outages and downtime causing delays,	Level 4. Significant consequence if outage occurs but capability for the	Unlikely	C



	inefficiencies and inability to operate and meet customers' expectations from the business	business to respond quicker given that mission critical systems are operable in response to the event, leading to less outage time.		
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.	Possible	C
R3.3	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 Higher risk where cyber vulnerability identified	C

**Table 12** below shows the costs of this option. While the costs of this option are higher than Options 1, due to the proactive refreshes for Business Critical applications, the risks of both energy network and business-wide disruption have significantly reduced.

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

Cost item	FY27	FY28	FY29	FY30	FY31	Total
Capex	\$8.9M	\$7.7M	\$9.9M	\$8.5M	\$10.7M	<b>\$45.7M</b>
Opex	\$0.7M	\$0.0M	\$0.3M	\$0.5M	\$0.5M	<b>\$2.0M</b>
Total	<b>\$9.6M</b>	<b>\$7.7M</b>	<b>\$10.2M</b>	<b>\$9.0M</b>	<b>\$11.2M</b>	<b>\$47.7M</b>

### 3.3. Option 3 – Proactive lifecycle refreshes for all systems

This option involves implementing a program of proactive lifecycle refresh across all systems, consistent with their vendor recommendations.

This option reduces the risk to as low as reasonably practical; minimising likelihood and consequences for all risks relative to Options 1 through 3. This can be seen in **Table 13** which includes lower risk of incidents resulting in disruption or inefficiency of specific business activities. This option will also proactively address the risks of cyber vulnerabilities from Business Operational & Administrative systems.

**Table 13 - Risk assessment of Option 3**

		Consequence					Legend
		1	2	3	4	5	
Likelihood	Almost certain			Material Risk threshold			
	Likely						
	Possible		R4.3	R4.2			
	Unlikely				R4.1		
	Rare						
							A
							B
							C
							D
							E

RISK	CONSEQUENCE	LIKELIHOOD	RISK RATING
R1	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.	Unlikely
			C

		Impact reduced as more limited potential for cascading dependency outages, and more timely response with vendor support		
R2	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	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 refreshes are required for all systems, but there is a reduction to opex from not having to manage any systems in-house. All risks to the distribution business are as low as practical.

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

Cost item	FY27	FY28	FY29	FY30	FY31	Total
<b>Capex</b>	\$9.6M	\$8.8M	\$11.5M	\$10.1M	\$11.4M	<b>\$51.4M</b>
<b>Opex</b>	\$0.7M	\$0.0M	\$0.3M	\$0.5M	\$0.5M	<b>\$2.0M</b>
<b>Total</b>	<b>\$10.3M</b>	<b>\$8.8M</b>	<b>\$11.7M</b>	<b>\$10.6M</b>	<b>\$11.9M</b>	<b>\$53.4M</b>

### 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 costs of this recommended option are \$45.7m capex and \$2.0m opex (\$real 2024), which represents a \$15.1m capex and \$1.7m opex 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
<b>Capex (\$million, real 2024)</b>	30.2	45.7	51.4	60.8
<b>Opex (\$million, real 2024)</b>	7.0	2.0	2.0	3.7
<b>Reduces risks below Material Risk threshold</b>	✗	✓	✓	✓
<b>Preferred option</b>	✗	✓	✗	✗

# 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](http://ausnet.com.au)

