AusNet

Transmission Revenue Reset

TRR (2027-32)

Digital Resilience - Applications

Friday, 31 October 2025

Table of contents

Executive Summary 4

1. Context 6

1.1 Role of digital systems for transmission 6

1.2 Historical trends 6

1.3 Approach to managing Digital Resilience risks 8

2. Identified needs 10

2.1 Drivers of investment 10

2.2 Approach to identifying needs 10

3. Options assessed 13

3.1. Assessment approach 13

3.2. Risk-cost assessment of options 13

3.3. Preferred option 18

Appendix A - Cost estimates of projects 19

Document history

DATE	VERSION	COMMENT
13/08/2025	V1.0	Initial draft business case for review
9/09/2025	V2.0	Revised business case incorporating input
6/10/2025	V3.0	Updated for final review
27/10/2025	V4.0	Final business case document

Related documents

DOCUMENT	VERSION	AUTHOR
Digital Resilience - Infrastructure Business Case	V4.0	AusNet Services
Technology Strategy and Investment Plan	V2.0	AusNet Services
Digital Program NPV Model	V2.0	AusNet Services

Approvals

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

Executive Summary

AusNet has over 200 technology systems and applications that enable delivery of an affordable and reliable electricity service to our customers. They support key functions such as operating our network securely and reliably, assisting efficient asset planning, and ensuring our business is run efficiently.

As a muti-utility, many of the applications are used across our electricity transmission and distribution networks, along with our gas distribution network, providing economies of scale. Our transmission services support all electricity customers in Victoria, and therefore the consequences of reliability or cyber incidents are most significant.

This business case is focused on "Digital Resilience" - maintaining the resiliency and capability from those technology applications we rely on to deliver transmission services. These investments represent recurrent expenditure per the AER ICT classifications.[1] Investments in new capability needs and associated options are detailed in companion business cases in AusNet's regulatory proposal.

The proposed recurrent capex is to manage resilience risks and cyber vulnerabilities from operating our digital applications. Technology systems are largely dependent on support from the product supplier (ie: vendors). Vendors often update their product to reflect changes in the market and will typically not support outdated versions. In the absence of vendor support, the systems and applications are more vulnerable to failing in service and to cyber-security risks.

AusNet's policy is to apply a criticality assessment approach to manage the cyber and resilience risks of digital applications. We categorise digital applications based on whether they are Mission Critical (high risk to energy system security), Business Critical (high risk of business wide disruption) or Business Operational and Administrative (risk to specific business functions). These criticality classification categories underpin our assessment of risk, and guide our approach to either proactively updating systems when vendors provide notice of upgrades or patches, or reactively undertaking updates on systems when vulnerabilities or functional risks are identified.

Our options assessment examined whether we should apply a proactive or reactive approach to each category of digital applications by examining the level of risk in the TRR 2027-32 period. We developed four options including not proactively updating any systems and reactively managing incidents when they arise, proactively updating Mission Critical systems only, proactively updating Mission Critical and Business Critical systems only, and proactively updating all systems. The preferred option was Option 3 on the basis of balancing required expenditure with mitigation of material risks. The results of the capex, opex and risk assessment is presented in **Table 1**.

Table 1 – Options assessment results ($m, real 2025, Transmission Network cost allocation)

OPTION	CAPEX	OPEX	RISK ASSESSMENT OUTCOME
Option 1: No upgrades for all systems, reactively managing the consequence of incidents	$18.8	$8.6	Results in high risk from system events and business-wide disruption, with risks above AusNet's material risk threshold
Option 2: Proactive lifecycle refresh on Mission Critical systems only, in-line with vendor recommendations	$27.8	$6.2	Results in high risk in terms of business-wide disruption, with risk above AusNet's material risk threshold
Option 3: Proactive lifecycle refresh on Mission and Business Critical systems, in line with vendor recommendations **(Recommended option)**	$33.6	$3.2	Mitigates key risks of system events and business wide disruption, with all risks within AusNet's material risk threshold
Option 4: Proactive lifecycle refresh and patching on all systems in line with vendor recommendations	$38.3	$1.6	Further mitigates risk of business inefficiencies, will all risks within AusNet's material risk threshold

[1] Australian Energy Regulator, Non-network ICT capex assessment approach, 2019, p8

The proposed program for the TRR 2027-32 period is $32.0 million of proactive capex ($real 2025) on Mission Critical and Business Critical system upgrades, and $1.6 million ($real 2025) on reactive capital expenditure for business operation and administration systems. **Figure 1** identifies forecast proactive capex on each application and system based, and assessed criticality. The most material program is the (C-I-C) upgrade to support the Advanced Energy Management System that provides real-time supervisory control, fault detection, isolation and service restoration, and outage management. The driver relates to the costs of migrating to the (C-I-C) in 2032.

All costs in this business case represent the cost apportioned to the transmission network business. For applications and systems that support multiple networks, we have allocated costs to each line of business based on AusNet's Cost Allocation Methodology (CAM) which is consistent with our recent Electricity Distribution Price Reset (EDPR) proposal. In some cases, expenditure is wholly allocated to transmission network, where the system is only used by AusNet's regulated transmission service.

Figure 1 – (C-I-C)

(C-I-C)

1. Context

Digitalisation has enabled AusNet to meet the growing challenges of providing reliable and secure transmission services to Victoria, and improving the efficiency of our services. Over the last decade, we have evolved our technology products to meet core functions and have continually scanned the market to provide the best value for money. The purpose of this section is to explain the role of digital systems in providing electricity transmission services, the evolution and journey of our technology ecosystem, and the current risk-based approach to supporting our systems including criticality categorising across mission critical, business critical, and business operational and administrative.

1.1 Role of digital systems for transmission

Our ICT applications comprise an integrated platform of technology systems and applications that support our network management and corporate functions. We currently operate over 200 ICT applications and systems.

The applications provide all manner of support functions to enable delivery of electricity for Victorians reliably and efficiently. Transmission services are provided to all Victorian customers, and therefore there is a greater consequence from a reliability or cyber incident. The applications enable AusNet to:

- Maintain power security – Our systems help us manage and control our network to ensure we can avoid widescale and extreme events, and improve our preparedness and response if these events occur.
- Improve safety and environmental outcomes – We have well developed systems to manage community and worker safety risks and environmental risks.
- Efficiently manage transmission assets – Our applications and systems improve the planning and decisions of our vital transmission network assets, ensuring we provide secure services at least cost to customers.
- Run an efficient and well-coordinated business – Our approach to integrate systems ensures that we meet our regulatory and corporate reporting obligations, and improve our analysis and decisions analytics.
- Communicate with key stakeholders – For our transmission business, this includes landholders particularly where we need to access land to ensure our assets are maintained appropriately.

AusNet's multi-utility structure provides opportunities to efficiently leverage many operational and business systems across multiple lines of business. For example, our enterprise systems such as SAP can be shared across our electricity transmission, distribution and gas lines of business, rather than requiring a stand-alone system. AusNet's Cost Allocation Methodology (CAM) is used to appropriately allocate costs for these shared systems between the lines of business. All costs described in this business case are those allocated to the transmission business, after the CAM has been applied.

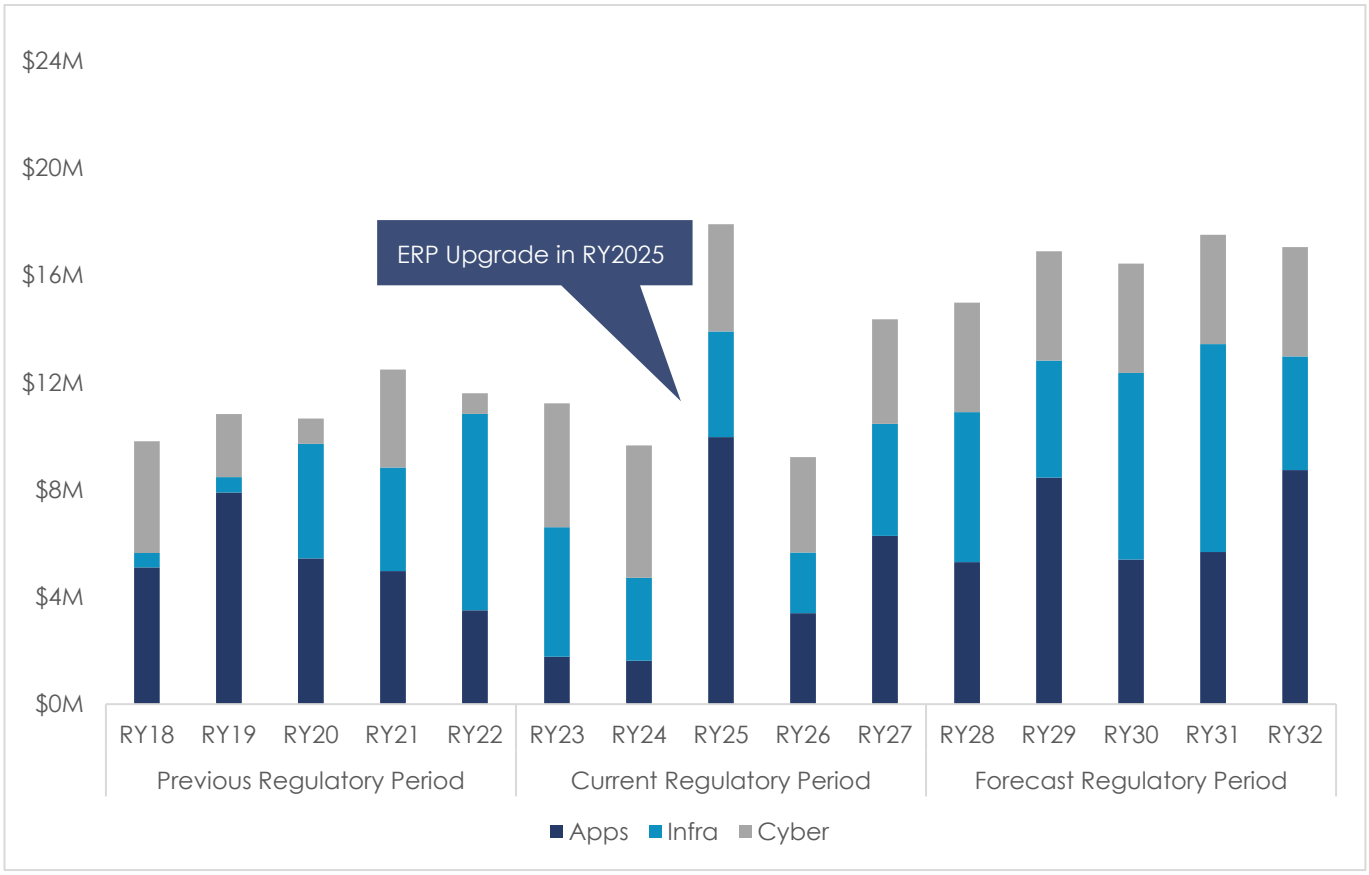
1.2 Historical trends

Figure 2 identifies our annual recurrent capital expenditure including applications, infrastructure, and cyber security.

In the current (RY2023-27) and previous (RY2018-2022) regulatory periods, we completed programs to proactively move a number of applications to cloud-based products, rather than renewing on premises, where this was assessed as prudent after taking into consideration system criticality and security, and the costs of migration and ongoing opex. This resulted in reduced application refresh costs over the RY2022 to RY2024 period. While no further focused cloud migration programs are planned in the coming period, we have noted a trend of some vendors to migrate their products to the cloud, requiring transition in order to maintain currency (even if not justified from a cost-benefit basis).

Outside of this period, recurrent applications refresh expenditure has averaged $5 to $6m per year ($real 2025) over the previous and current regulatory period. Lifecycle upgrade of ERP system resulted in peak expenditure in RY2025. AusNet's proposal will see application refresh expenditure continue at the c.$6m per year level in the coming period, with variability across years driven by application and system refresh timing.

Figure 2 – Recurrent transmission expenditure on ICT applications, infrastructure and cyber security ($m, real 2025)



1.3 Approach to managing Digital Resilience risks

AusNet's policy is to apply a system criticality approach to manage the resilience risks of our applications and systems. This approach prioritises proactive management of the resilience and cyber risks posed on our most critical applications and systems, consistent with the risk consequence and likelihood of impact. This informs our approach to the timing of vendor updates and patching activities.

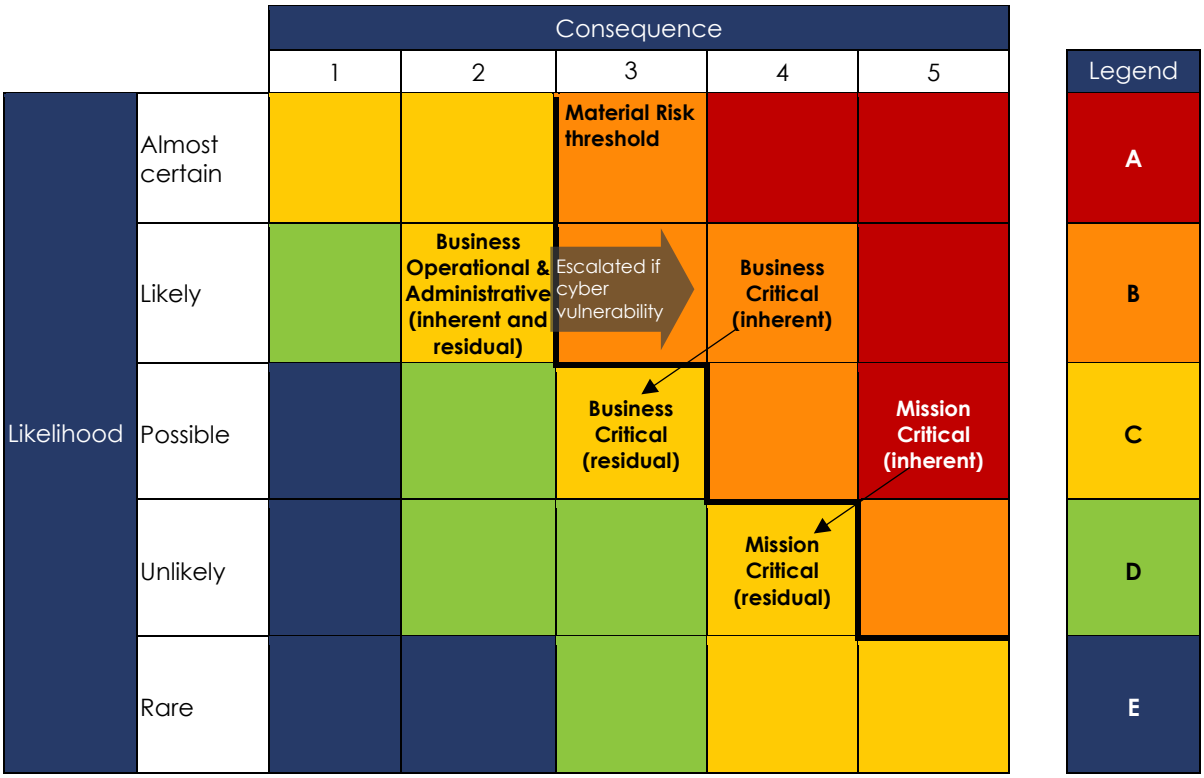
Through 2025 we have enhanced this criticality assessment and risk management framework, resulting in applications and systems being classified into three categories. These criticality classification categories underpin our assessment of risk, in terms resilience and cyber security, posed by the applications and systems. These categories also guide our approach of either proactively updating when vendors provide notice of upgrades or patches, or reactively undertaking updates on systems when vulnerabilities or functional failures are identified. These criticality categories and AusNet's risk management approach are detailed below.

- **Mission Critical** (proactive) – These are applications and systems that are essential to providing electricity to Victoria as defined by the risk of significant NEM disruption from a widescale 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) – 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) – These are systems that while important for ongoing business function and efficiency, they are not directly related to the energy network operability and an outage would not create widescale business disruption. Our approach for these systems is to reactively manage 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 3 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 upgrade if required to mitigate.

Figure 3 – Risk assessment of Mission Critical, Business Critical and Business Operational & Administrative systems



2. Identified needs

The purpose of this section is to identify the overarching driver of recurrent capex in technology systems and applications, and to pinpoint our approach to identifying investment needs across our suite of technology assets.

2.1 Drivers of investment

The overarching driver for investment is to reduce the risk posed by our digital applications and systems failing in service or giving rise to cyber-security threats. This is achieved through criticality and risk-based maintenance of system currency to provide required resiliency. Unlike network assets, technology assets have a short technical life and are much more dependent on the support from the initial supplier (ie: vendor) to provide support and ongoing product updates to address defects or security vulnerabilities. To this end, vendors often update their product to reflect changes in the market and will typically not support outdated versions. In addition, applications and systems require patching and bug-fixes to maintain performance and security.

As such the recurrent investment is to maintain existing capability by updating our applications and systems to provide continued vendor support:

- Technology applications require vendor support – Extending the life of technology applications after the vendor end of life date increases network operational and business risk as the likelihood of failure increases. The stability of applications is maintained through application refreshes.
- Vendors continually update their products – Vendors periodically release updated versions of their products to ensure they remain current to the market and improve effectiveness over time.
- Vendors may not provide support for out-dated versions – It becomes uneconomic for vendors to provide support for outdated applications, due to decreasing customer base. This cost is passed on to the customer and often exceeds the cost of deploying and maintaining new applications.
- Unsupported systems are more vulnerable to failure and cyber security risks – Unsupported systems pose a higher risk of failure and from cyber-security vulnerabilities. When applications are no longer supported by a vendor, no new patches are made available to address security vulnerabilities. The risk of unauthorised access leading to loss of service, data loss, or non-compliance with regulatory requirements, increases over time.

2.2 Approach to identifying needs

Our approach to identify needs was to determine the known or likely timing of vendor updates to each of our existing applications and systems, by their assessed criticality level. In some cases, we did not have exhaustive bottom-up information on upcoming vendor upgrades given that we are forecasting to 2032. In these cases, we sought to apply an estimate of the likely vendor update cycle which is generally about 5 years.

Our identification of needs also sought to identify whether there remained a continued business need for the application or system. This considered whether the function may be provided through a planned non-recurrent ICT investment.

Table 2 sets out the list of Mission Critical systems, Business Critical systems and Business Operational & Administrative systems requiring update investments in the TRR 2027-32 period. We identify the application / system function, and the vendor product requiring recurrent capex to address resilience risks.

Table 2 – System, function and vendor product

System or application	Description of function	Vendor product
Mission critical systems		
SCADA and Advanced Energy Management System (AEMS)	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)
Telecommunications Systems	AusNet utilises telecommunication systems which support SCADA to communicate network state and performance of assets and to respond to emergencies.	(C-I-C)
Identity Management	For security purposes, AusNet has a system that enables core identity and access to systems. The system provided functions such as single sign on and two factor authentication for employees and contracts which require access to AusNet systems.	(C-I-C)
Other mission critical transmission applications	Our control centre uses a series of telephone tools that support active and backup communication to AEMO and the Terminal Substations that are mission critical.	(C-I-C)
Business critical systems		
Enterprise Resource Planning (ERP)	AusNet uses an ERP to manage business transactions and data across business functions in a single integrated system. This includes finance, human resources, procurement, asset management, and works management.	(C-I-C)
Geospatial Systems	AusNet uses Geographic Information Systems 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	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)
SCADA Data Historian	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	Ausnet uses applications that provides solar irradiance and weather data from data providers which are integrated into various systems to ensure the reliability and security of the distribution network and for forecasting purposes	(C-I-C)
Protection and Control Settings	AusNet uses power system modelling software for secondary protection settings and DFA schemes	(C-I-C)
Other Business Critical transmission systems	This includes an array of critical business systems for the transmission business e.g. access control, protection schemes, workstations	(C-I-C)
Business Operational & Administrative		

Data and Analytics	AusNet uses an on-cloud enterprise data warehouse which aggregates data from many different sources into a central and consistent data repository to support data analysis and reporting.	(C-I-C)
Health Safety Environment and Quality	Ausnet uses systems to track, monitor and report on Health, Safety, Environment and Quality functions including risk management.	(C-I-C)
Other operational business systems	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	(C-I-C)

3. Options assessed

The purpose of this section is to identify the options we have considered in developing our proposed program of recurrent capex for the TRR 2027-32 period for applications and systems.

3.1. Assessment approach

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

The AER identifies three approaches to assess recurrent expenditure. In terms of bottom-up analysis, the AER recognises that recurrent expenditure relates to maintaining an existing service and that it will not always be the case that the investment will have a positive NPV. It expects that a business case will consider possible multiple timing and scope options of the investments (to demonstrate prudency) and options for alternative systems and service providers (to demonstrate efficiency). The AER also assess the program as a whole including whether the proposed expenditure varies from historical trends, and benchmarking analysis compared to peer networks.

To give effect to this methodology we undertook risk and cost analysis of options to updating our current systems and applications. This involved understanding the full extent of the risk of 'doing nothing' and testing whether alternative approaches to updating Mission Critical, Business Critical and Business Operational & Administrative systems would be justified on a risk-cost basis as set out in Sections 3.2 and 3.3.

3.2. Risk-cost assessment of options

We used risk-cost analysis to determine the optimal strategy for recurrent applications expenditure as set out in **Table 3**. We analysed four options that included a decision on whether to proactively refresh systems with current updates and patching, or reactively manage the risks of not performing currency updates and patching.

We analysed the relative risk of reactively managing risks for all systems (Option 1), proactively refreshing Mission Critical systems only (Option 2), proactively refreshing Mission and Business Critical systems (Option 3), and proactively refreshing all systems across all assessed criticality (Option 4).

Table 3 – Options evaluated for applications and systems digital resilience

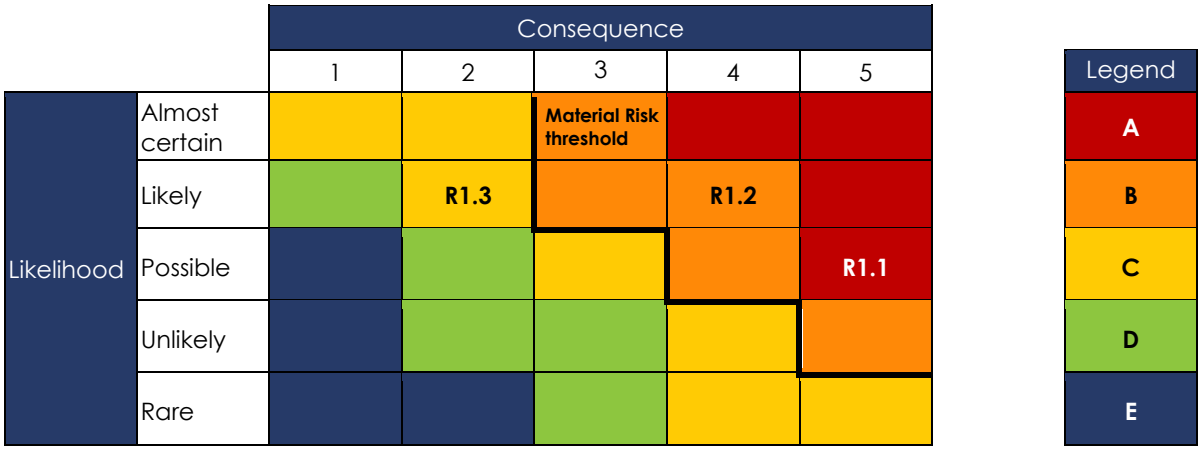
OPTION	SUMMARY
Option 1: No upgrades for all systems, reactively managing the consequence of incidents	Run our existing stock of applications and systems without performing any updates or patching. Reactively manage resilience exposures and cyber vulnerabilities for all systems in-house, through operational expenditure directed at mitigating the consequence of the incident, and capital expenditure if the mitigating action requires an upgrade.
Option 2: 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.
Option 3: Proactive lifecycle refresh on Mission and Business Critical systems, in line with vendor recommendations **(Recommended option)**	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.
Option 4: 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.

3.2.1. Option 1 – Reactively manage all systems

Under this option, we would operate our technology systems without undertaking periodic refreshes. We would expect a higher occurrence of cyber threats, system failures and other incidents. This would require reactive support within the business resulting in higher operational expenditure. This would also necessitate capital expenditure on upgrades or patching in cases where an upgrade is required to minimise consequences or to mitigate a revealed cyber vulnerability. We note that cloud applications would continue to be supported by vendors.

There is a high level of risk associated with this option. **Table 4** shows the risk matrix relative to which we have assessed each of risks within the options. Risks of highest concern are rated red, whereas those of lowest concern are rated blue. The risks for this option are consistent with the inherent risks detailed in Section 1.3 and are above AusNet's material risk threshold.

Table 4 - Risk assessment of Option 1



	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 5. Inoperable Mission Critical systems impacts the ability to detect and respond to potential system failures and station blacks. Significant scale of impact to Victoria from no power supply	Possible	A
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.	Likely	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 Higher risk where cyber vulnerability identified	C

Costs for this option are shown in **Table 5** 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 5 - Forecast expenditure for Option 1 ($million real 2025, transmission network allocated costs)

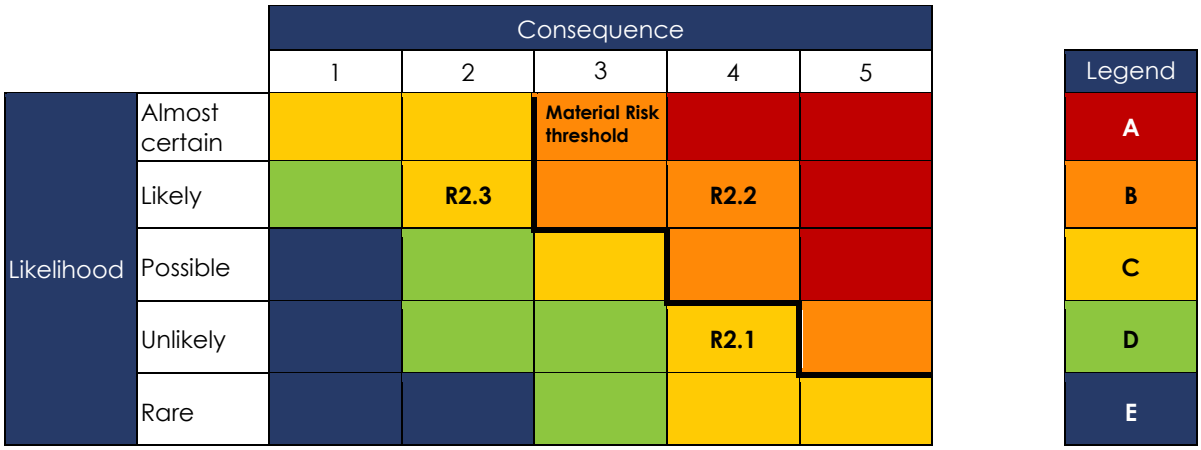
Cost item	RY28	RY29	RY30	RY31	RY32	Total
Capex	$3.06	$3.90	$2.58	$3.36	$5.87	**$18.77**
Opex	$1.52	$2.13	$1.75	$1.46	$1.73	**$8.59**
Total	**$4.59**	**$6.03**	**$4.33**	**$4.82**	**$7.60**	**$27.36**

3.2.2. Option 2 – Proactive refreshes on Mission Critical systems only

This option seeks to perform proactive lifecycle refreshes and patches on all Mission Critical systems (e.g. the e-terra SCADA system, identity management and telecommunications systems). This reflects the criticality of these systems in terms of consequences to energy security in Victoria. Under this option, Business Critical and Business Operational & Administrative systems would be actively reactively managed consistent with Option 1 above.

As can be seen from **Table 6** below, the risks are lower than Option 1 for energy system failures or station events with a reduction in consequence. For example, the SCADA system is 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 6 - Risk assessment of Option 2



	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. 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
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.	Likely	C Higher risk where cyber vulnerability identified

Table 7 below shows the costs of this option. Capex is higher than Option 1 due to the refreshes for Mission Critical systems, with a reduction to opex from not having to manage these systems in-house. Overall, the costs are higher than Option 1, however there is a reduction in the resilience risks of Mission Critical systems.

Table 7 - Forecast expenditure for Option 2 ($million real 2025, transmission network allocated costs)

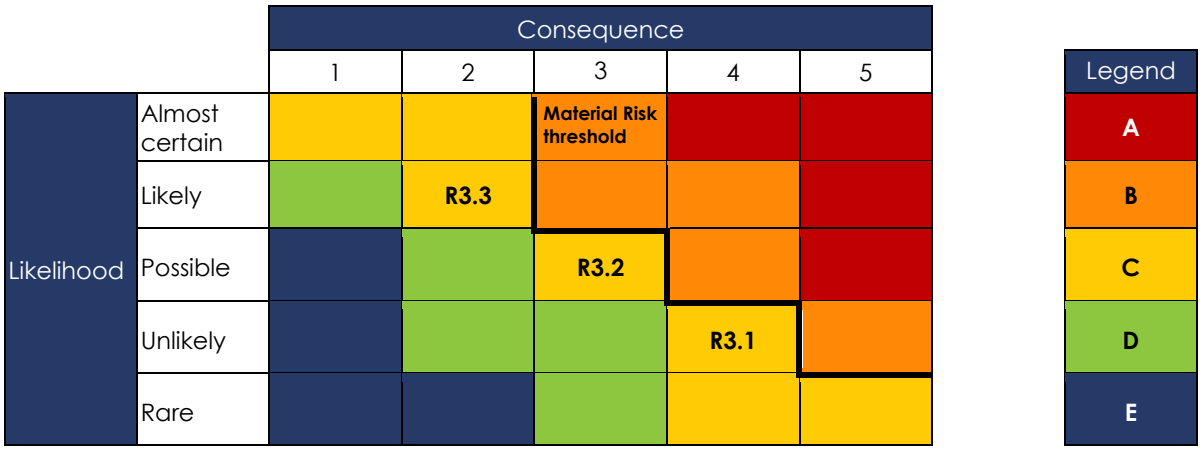
Cost item	RY28	RY29	RY30	RY31	RY32	Total
Capex	$4.57	$5.24	$4.29	$5.32	$8.33	$27.76
Opex	$0.98	$1.78	$1.31	$1.00	$1.13	$6.20
Total	**$5.55**	**$7.02**	**$5.60**	**$6.32**	**$9.46**	**$33.96**

3.2.3. Option 3 – 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 8**, 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 8 - Risk assessment of Option 3



	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. 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
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 9 below shows the costs of this option. Capex is higher than Option 1 and 2 due to the refreshes for Business Critical systems and opex marginally reduces. Recognising the trend of some vendors to move newer application versions solely to the cloud, the cost of this option includes opex to account for these forced cloud migrations, along with opex for reactive management of Business Operational & Administrative systems. While the costs of this option are higher than Options 1 and 2, the risks of both energy network and business-wide disruption have significantly reduced.

Table 9 - Forecast expenditure for Option 3 ($million, real 2025, transmission network allocated costs)

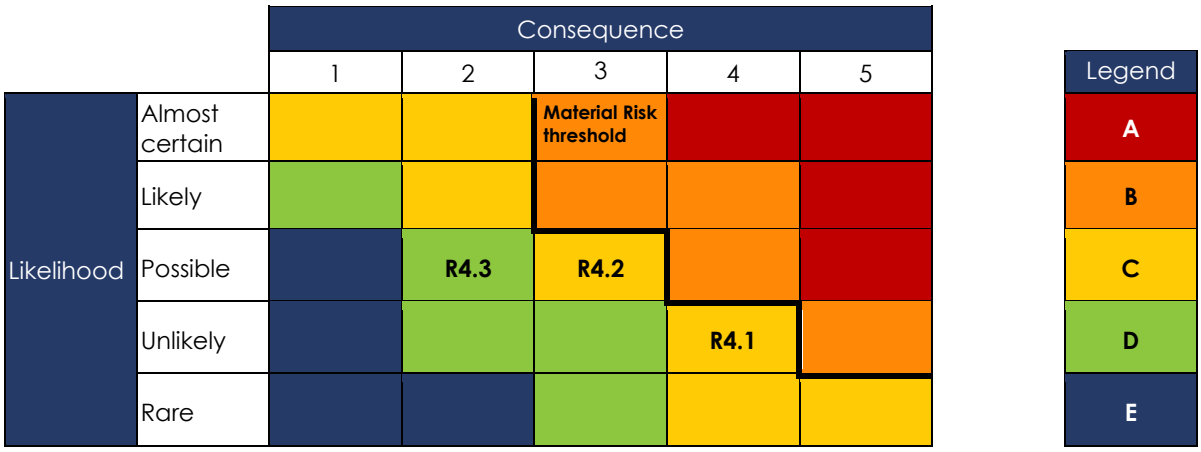
Cost item	RY28	RY29	RY30	RY31	RY32	Total
Capex	$5.30	$8.45	$5.40	$5.67	$8.74	**$33.56**
Opex	$0.51	$0.53	$0.60	$0.70	$0.81	**$3.15**
Total	**$5.81**	**$8.99**	**$6.00**	**$6.38**	**$9.54**	**$36.72**

3.2.4. Option 4 – 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 to 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 10** 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 10 - Risk assessment of Option 4



	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. Impact reduced as more limited potential for cascading dependency outages, and more timely response with vendor support	Unlikely	C
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 11 below shows the costs of this option. Capex is higher than Option 1, 2 and 3 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 transmission business are as low as practical.

Table 11 Forecast expenditure for Option 4 ($million, real 2025, transmission network allocated costs)

Cost item	RY28	RY29	RY30	RY31	RY32	Total
Capex	$6.52	$9.42	$6.25	$6.52	$9.58	**$38.30**
Opex	$0.41	$0.32	$0.28	$0.28	$0.28	**$1.58**
Total	**$6.93**	**$9.75**	**$6.53**	**$6.81**	**$9.87**	**$39.88**

3.3. Preferred option

Our assessment found that Option 3, proactive refreshes for Mission Critical and Business Critical applications and systems, is the preferred option. This option most cost effectively manages digital resilience risks within AusNet's Material Risk threshold as shown below.

Criteria	Option 1	Option 2	Option 3	Option 4
Capex ($million, real 2025)	18.8	27.8	33.6	38.3
Opex ($million, real 2025)	8.6	6.2	3.2	1.6
Reduces risks below Material Risk threshold	✗	✗	✓	✓
Preferred option	✗	✗	✓	✗

The costs of this recommended option are $33.56m capex and $3.15m opex, as shown in **Table 12** below. These costs represent those allocated to the transmission business, after application of AusNet's Cost Allocation Methodology for applications and systems shared across multiple networks.

Table 12 Forecast expenditure for Option 3 ($million, real 2025, transmission network allocated costs)

Cost item	RY28	RY29	RY30	RY31	RY32	Total
Capex	$5.30	$8.45	$5.40	$5.67	$8.74	**$33.56**
Opex	$0.51	$0.53	$0.60	$0.70	$0.81	**$3.15**
Total	**$5.81**	**$8.99**	**$6.00**	**$6.38**	**$9.54**	**$36.72**

Appendix A - Cost estimates of projects

Table 9 sets out the cost estimates for each application or system. This has been based on either the known or estimated costs of maintaining support, consistent with the preferred option in Section 3.3.

Note that all amounts represent capex allocation to electricity transmission business, after application of AusNet's Cost Allocation Methodology (CAM) where systems are shared across networks.

Table 13 – (C-I-C)

(C-I-C)

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