AusNet

Transmission Revenue Reset TRR (2027-32)

Digital Resilience - Infrastructure

Friday, 31 October 2025

Table of contents

Document history

DATE	VERSION	COMMENT
20/08/2025	V1.0	Initial draft business case for review
18/09/2025	V2.0	Revised business case incorporating input
23/10/2025	V3.0	Updated for final review
30/10/2025	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

ICT infrastructure includes compute servers, storage servers, telecommunications and end user devices. Infrastructure is the foundation to operating the technology systems that enable AusNet's capability to securely control the Victorian transmission network, efficiently plan and maintain assets, and efficiently run our business. For this purpose, AusNet owns and operates ICT infrastructure 'on premise' in our Richmond and Rowville data centres. This 'on premise' infrastructure underpins transmission services to all Victorians.

This business case is focused on "Digital Resilience" - maintaining the resiliency and capability of the ICT infrastructure that we rely on to deliver transmission services. These represent recurrent capex 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 infrastructure. This includes undertaking life cycle refreshes of hardware such as compute and storage servers, refurbishing data centre facilities such as air conditioners, refreshing telecommunications infrastructure, and replace end user devices such as laptop computers.

AusNet applies a criticality-based approach to manage resilience and cyber risks across its digital infrastructure. Assets are classified as 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 classifications guide whether infrastructure is proactively refreshed at end of life / support or reactively replaced when vulnerabilities or failures occur. We define end of life / support by the end of vendor mainstream support or warranty, end of extended support, loss of patch/parts availability, or failure. These differing definitions influence AusNet's responsiveness and have been considered in our program options assessment.

We evaluated four options for managing infrastructure risks during RY2028–32:

- Option 1 – reactive approach, replacing only upon failure or vulnerability
- Option 2 – proactively upgrade Mission Critical infrastructure to remain within vendor extended support
- Option 3 – proactively upgrade Mission and Business Critical infrastructure to remain within vendor extended support
- Option 4 – proactively upgrade all infrastructure to remain under vendor mainstream support

The summary results of the assessment of these options are detailed in **Table 1** below.

Table 1 – Options assessment results ($m, real FY2025)

OPTION	CAPEX	OPEX	RISK ASSESSMENT
Option 1: No proactive refresh to infrastructure, over the next 5-year period. Less infrastructure will be vendor supported and incidents will increase (i.e. a run to failure).	$14.0	$10.1	Results in high risk from system events and business-wide disruption, with risks above AusNet's material risk threshold. Depending on the timing of the failure this may trigger a vendor supported warranty replacement, fix through access to spares or replacement with new equipment.
Option 2: Proactive lifecycle refresh on Mission Critical infrastructure only, leveraging vendor extended support arrangement and patch/parts availability.	$16.7	$8.5	Address Mission Critical infrastructure risks. Results in elevated risk of business-wide disruption related to business critical, operation and administrative systems, with risk above AusNet's material risk threshold.
Option 3: Proactive lifecycle refresh on Mission and Business Critical infrastructure, leveraging vendor extended support arrangement and patch/parts availability. **(Recommended option)**	$28.9	$0.3	Mitigates key risks of system events and business wide disruption, with minor disruptions related to operation and administrative systems. All risks within AusNet's material risk threshold

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

Option 4: Proactive lifecycle refresh of all infrastructure and maintain with vendor mainstream support.	$46.6	$0.0	Further mitigates risk of business inefficiencies or ineffectiveness due to infrastructure failures, wilth all risks within AusNet's material risk threshold. Reduces the likelihood or duration of the outage as vendor responsiveness SLAs are better during mainstream support.

From this assessment Option 3 is preferred, as it best balances cost with mitigation of material energy security and business disruption risks. Under this approach, infrastructure will operate until the end of vendor extended support, leveraging patch and parts availability to maximise asset value, while user devices will be managed reactively upon failure.

The proposed program for the RY2028-32 regulatory period is $28.9million ($real 2025). This consists of $28.7m ($real 2025) for lifecycle refreshes of hardware and infrastructure within the data centre, telecommunications upgrades, and facility management of the data centres including fire suppression equipment and air conditioning. We have also included $0.2 million of capex for reactive upgrades of user devices when incidents are logged, rather than to undertake periodic replacement which would have cost $1.2 million capex.

Figure 1 identifies forecast recurrent capex on each infrastructure areas of this program. Shared data centre infrastructure and upgrades to the high security network are the most material contributors to the capital program. Shared data centre infrastructure comprises the servers and storage used to operate AusNet's applications and systems. The high security (or "HiSec") network is the telecommunications network infrastructure that supports communications to depot and terminal substations.

All costs in this business case represent the cost apportioned to the transmission network business. For infrastructure 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, our expenditure is solely for transmission services where the infrastructure is solely related to a transmission system or application.

Figure 1 (C-I-C)

1. Context

Digital technologies are integral to supporting a secure power system and enabling the business to perform its functions efficiently. ICT infrastructure provides the processing capacity to analyse and retrieve data, store information, communicate between systems and devices, and includes laptops and other end user devices to enable our organisation's work.

ICT infrastructure is a critical enabler of our ecosystem of ICT applications and systems. The applications provide a critical support function to deliver our transmission network services reliably and efficiently across Victoria.

1.1 Categories of ICT infrastructure

The scope of this business case relates to ICT infrastructure on premises used to support our applications and systems. ICT infrastructure includes:

- **Hardware** – Servers are housed in racks in a data centre. Compute servers provide the necessary computing power and resources to run AusNet's applications and systems for end users. Storage servers provide a centralised location for storing and retrieving information, making it accessible to authorized users from various locations.
- **Telecommunications infrastructure -** This encompasses the network components and systems that enable secure, reliable communication across AusNet's operational footprint. It includes fibre cabling with multiplexers, microwave radio towers and receives for redundant communication paths, switches, routers, and firewalls that interconnect substations with our control centres to support real-time monitoring and management of the transmission network. These assets also provide critical pathways for emergency management communications, ensuring resilience and continuity during incidents or outages.
- **Data centre facilities** – Data centres are physical facilities that houses IT infrastructure for building, running and delivering applications and services. We have two data centres on premises in Richmond and Rowville that are used to support the operating technology applications and systems for AusNet's transmission and distribution electricity networks.
- **End user devices** – This includes equipment used directly by our staff to perform their work activities including laptops, mobile and landline phones, field devices, Regional Mobile Radios (RMR) and printers. In a modern workplace, this suite of digital tools are required to perform our underlying functions effectively and efficiently. Generally, these assets have a supported life of about 3 to 5 years.

1.2 Drivers of investment

The overarching driver for investment is to ensure our ICT infrastructure is functional and operational to support our applications and systems. Unlike software, ICT infrastructure assets such as servers and network communications are largely generic and, with appropriate virtualisation and management software, can support multiple applications and systems.

We scale our infrastructure to meet the demands for processing and storage for all our applications and systems, purchasing sufficient racks, servers, and communication networks to deliver adequate performance. When we purchase infrastructure from vendors, we generally enter into a maintenance support agreement which effectively provides a warranty for the expected life of the asset. We may be provided with the opportunity to purchase extended support, and this option is typically taken where financially prudent.

At the end of the extended support period, there is a higher risk that the asset will fail in service. The availability of parts for direct replacement to address the failure becomes less likely, which impacts the time it takes to address the infrastructure outage. Applications and systems would not be able to operate at all or at required performance until the infrastructure is replaced, ultimately giving rise to significant risks to AusNet's ability to deliver its' network and support functions.

As detailed in Section 1.4, AusNet applies a system criticality and risk framework to the management of infrastructure lifecycle risks. Per this framework, and consistent with other networks, AusNet seeks to refresh and replace its critical infrastructure within the extended support periods offered by vendors, leading to periodic cycles of renewal investment.

This lifecycle varies by infrastructure type, and this has been reflected in the refresh cycle. The lifecycle is typically dictated by the vendor release date of that hardware series. For servers, vendors typically offer 5 years of mainstream support with an additional 2 years of extended support, storage is typically 7 years of mainstream support with 2 years extended support, network equipment is typically 5 years of mainstream support with 5 years extended support.

1.3 Historical expenditure

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

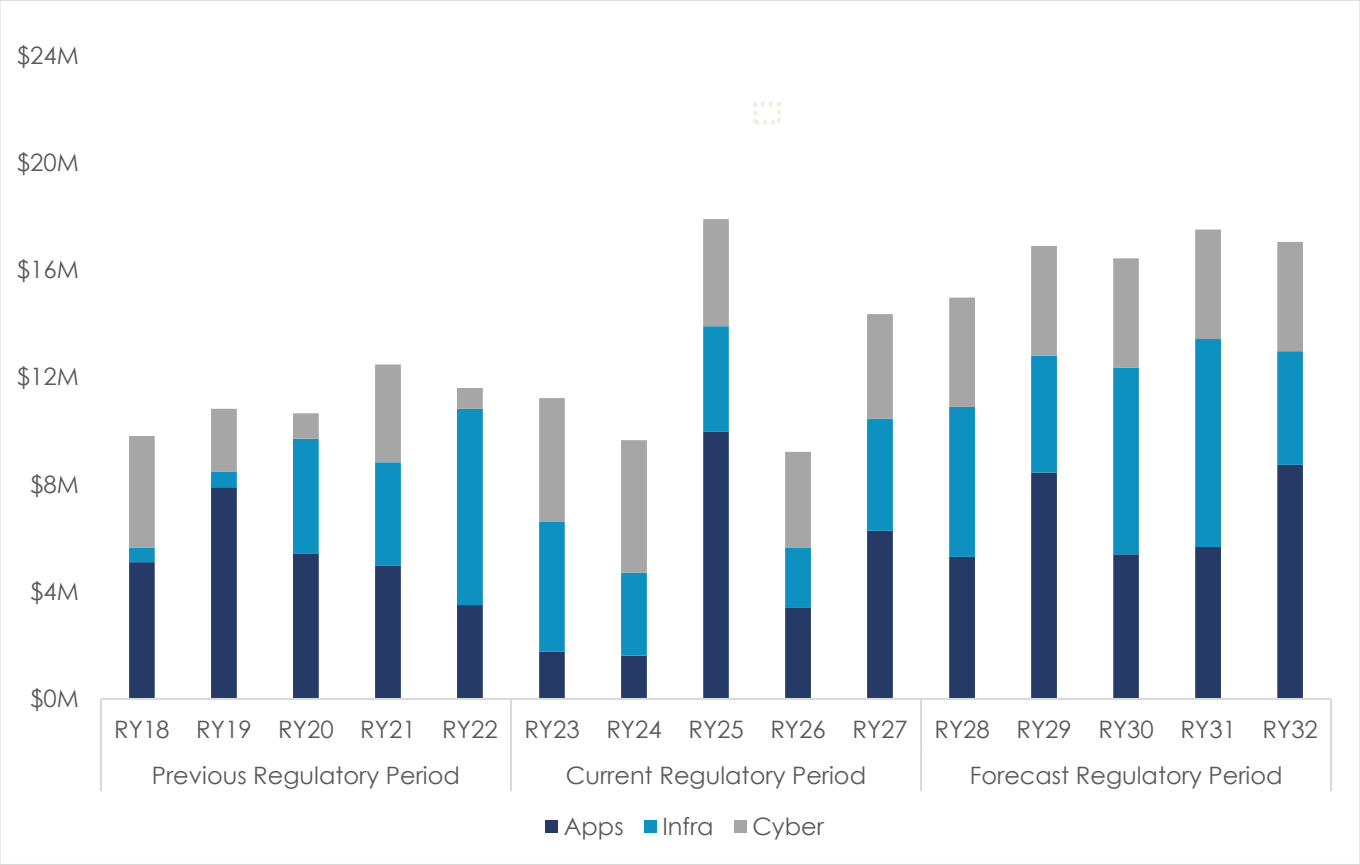
AusNet's ICT infrastructure architecture has evolved with technology improvements and business needs. Over the past 10 years we have consolidated our ICT infrastructure to two data centres. The decision to host operating technology infrastructure on premises largely relates to the performance, operational resilience and cyber security needs of our electricity networks.

In the RY2023-27 period we examined options to move infrastructure services to the cloud, in line with broader technology maturity opportunities. Our assessment was that keeping operating technology infrastructure in-house was appropriate for applications and systems that were Mission Critical to the operation of the transmission network, and minimised risks by providing more control over these systems. However, we found opportunities to move less critical applications to the cloud to access industry innovation.

Over the past 5 years recurrent infrastructure expenditure has averaged $4m to $7m per year ($real 2025). AusNet's proposal will see annual infrastructure refresh expenditure continue in this range in the coming period, with variability across years driven by the timing and scope of required upgrades.

With overall recurrent capex remaining relatively consistent over this period, this demonstrates the effectiveness of AusNet's balancing and optimisation between on-premises and cloud implementations, and that AusNet's procurement strategies are enabling us to obtain good value for money from our vendors when acquiring replacement infrastructure and that we continue to keep pace with efficiencies in technologies.

Figure 1 – Recurrent transmission expenditure on ICT applications, infrastructure and cyber security ($m, real 2025)



1.4 Approach to managing Digital Resilience risks

Digital Infrastructure Criticality and Lifecycle Management

AusNet applies a system criticality-based approach to manage the resilience and cyber risks across our digital infrastructure. This framework ensures resources and investment are prioritised toward infrastructure that supports the safe and reliable delivery of electricity to Victoria, consistent with the likelihood and consequence of potential failures. This approach guides our approach to the timing of hardware refreshes and upgrades.

Criticality Assessment and Risk Management Framework

Through 2025, AusNet enhanced its 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 Victoria, where failure could cause significant disruption to the National Electricity Market (NEM).

- 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 system security or business continuity.

- Example: User devices such as laptops and desktop computers.
- Approach: Manage upgrades reactively 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

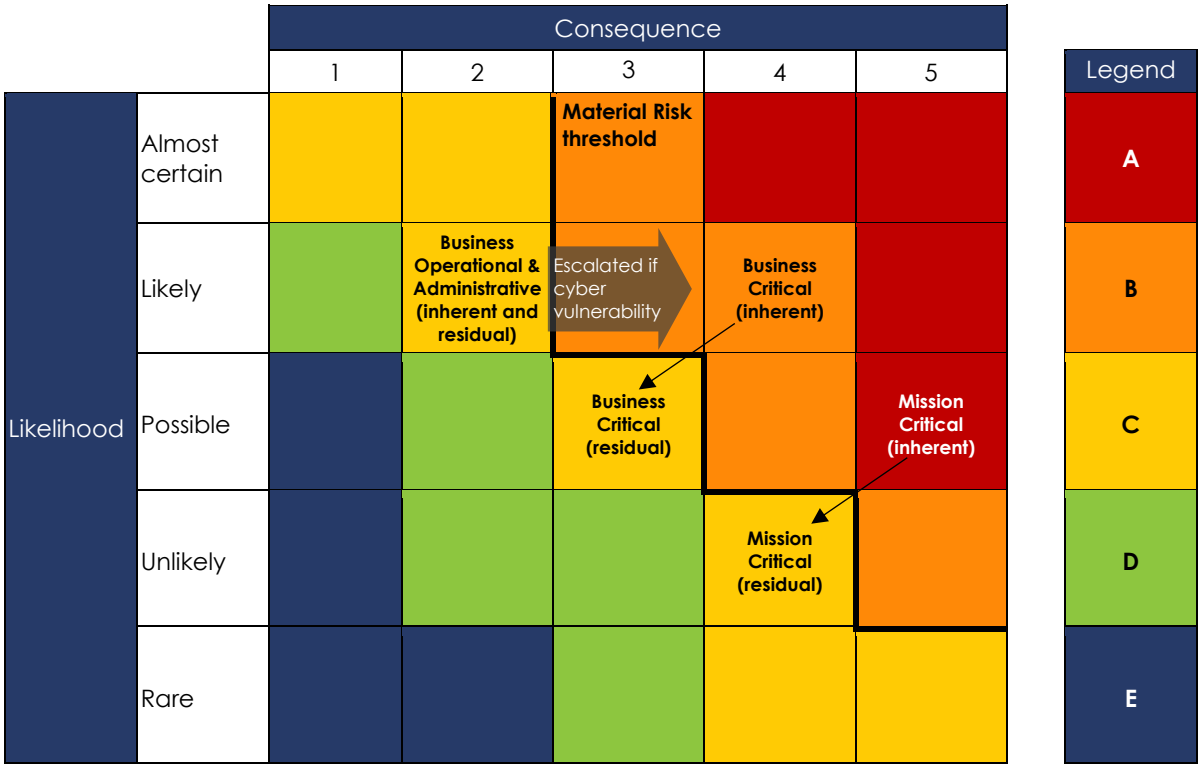
AusNet's preferred lifecycle approach is to replace assets just before the end of extended support, ensuring cost-effective resilience and alignment with industry best practice.

- 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 3 illustrates how this life cycle strategy aligns to our Enterprise Risk Management model. It shows how inherent risk (without mitigations) and residual risk (with implementation 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 Victoria's electricity network.

Figure 2 – Risk assessment of Mission Critical, Business Critical and Business Operational & Administrative infrastructure



2. Needs identification

The purpose of this section is to identify the forecast methods and components of the proposed recurrent infrastructure capex program, and to demonstrate why it is efficient and prudent.

2.1 Optimal infrastructure environment

Our starting point for developing our forecast for the RY2028-32 period was to assess whether there were any improvements we could make to the way we manage our ICT infrastructure services.

As noted in Section 1.3, AusNet has consolidated and optimised its mix of cloud and on-premise infrastructure over the past 10 years. We have found opportunities to migrate non Mission Critical applications and systems to the cloud, where we want to access industry innovation. However, our experience is that on-premises infrastructure is essential to maintaining control of Mission Critical connectivity across our transmission network, guaranteeing protection of communication paths that require deterministic traffic.

In the RY2028-32 regulatory period, we will examine ways to fine-tune performance of our data centres by moving towards 'private cloud' architecture arrangements. Currently, AusNet's data centre hosts isolated servers and storage dedicated to specific applications and systems. In turn, this limits opportunities to substitute infrastructure where the need arises. A private cloud enables perfect substitution for servers and storage, and could result in more efficiencies if adequately provisioned and managed. Our budgets for the RY2028-32 period reflect such optimisations of the existing infrastructure.

2.2 Approach to identifying needs

As discussed in section 1.4, our approach is to undertake lifecycle refreshes of Mission Critical and Business Critical infrastructure in line with vendor recommendations and extended support periods. This is consistent with the general practice of other transmission networks, given the criticality of ongoing support for infrastructure. We continue to analyse whether there are opportunities to adopt the "out of extended support" (run to failure) on selective infrastructure assets with lower impact of failure. Importantly, we have externally tendered for infrastructure equipment where we consider the lowest lifecycle costs, by leveraging the vendor extended support offerings, to meet our needs.

Our capital expenditure forecasts for the RY2028-32 period are based on vendor extended refresh timing and guidance, where known, and operating experience-based assessment of replacement cycles and costs for our existing infrastructure. Granular assessment of infrastructure replacement needs out to 2032 is challenging so far in advance.

Our identification of needs also sought to identify whether there remained a continued business need for infrastructure, with consideration to whether non-recurrent needs may meet the recurrent need.

Table 2 sets out the proposed capital expenditure in the RY2028-32 period for ICT infrastructure.

Table 2 – Underlying need for infrastructure ($ million, real 2025)

Infrastructure type	Description of need	Cost
Mission critical infrastructure		
Mission – Other infrastructure upgrades	This includes the infrastructure to support a range of mission critical applications such as (C-I-C), etc that enable AEMO and field communication with the control room.	(C-I-C)
Telecommunications Systems hardware	This includes refreshing and supporting the equipment in the data centres required for system that manage the SCADA communicate to field device, e.g. (C-I-C).	(C-I-C)
Fire suppression	This is to ensure the data centres have appropriate fire protection measures to ensure the safety and security of the data centre and the infrastructure that is required to support critical applications. This includes phase out of legacy fire suppression gases consistent with regulatory requirements.	(C-I-C)

Data centre facilities	Includes maintenance and upgrades to the CRAC (computer room air-conditioning) units and the uninterrupted power system.	(C-I-C)
Business critical infrastructure		
High security network	This involves refreshing the telecommunications and IT network infrastructure that supports communication to depot and terminal substation for non-SCADA operations.	(C-I-C)
Shared Data Centre Infrastructure	The 2 data centres require continual refreshes to ensure that storage, servers and other computing equipment provide the necessary support for the current suite of applications and systems.	(C-I-C)
SCADA Data Historian Infrastructure	The infrastructure and storage required to operate the (C-I-C) (SCADA Data Historian).	(C-I-C)
Business - Other infrastructure upgrades	This includes the infrastructure to support various business applications such as (C-I-C)	(C-I-C)
System Integration Platforms infrastructure	Infrastructure that supports the Enterprise Application Integration platforms including (C-I-C)	(C-I-C)
Physical security digital infrastructure	Infrastructure required to run security cameras, building access control (gates) systems, etc. This includes service, network and storage. Support the high speed and volume of storage required for the security video footage collected.	(C-I-C)
OT Communication equipment firmware	Periodic firmware updates to field OT Communication equipment to maintain vendor support, ensure new elements can be installed within the lifecycle parameters, provide cyber security coverage through pen testing and vulnerability scanning.	(C-I-C)
Business Operational & Administrative		
User Devices (laptops, mobile, peripherals)	Extended refreshes of workstations, laptops, mobiles and other end user devices.	(C-I-C)

3. Options consideration

The purpose of this section is to identify the options we have considered in developing our proposed program of recurrent capex for the RY28-32 period for infrastructure.

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 the following approach to develop a prudent and efficient program for our existing infrastructure. We undertook risk and cost analysis of options to updating our current infrastructure, involving understanding the full extent of the risk of 'doing nothing' and testing whether an alternative approach of refreshing Mission Critical, Business Critical and Business Operational & Administrative infrastructure would be justified in terms of risks and costs.

3.2. Risk-cost assessment of options

We used risk-cost analysis to determine the optimal strategy for recurrent expenditure on infrastructure as set out in **Table 3**. We analysed the relative risk and costs of reactively managing risks for all infrastructure (Option 1), proactively refreshing Mission Critical infrastructure only (Option 2), proactively refreshing Mission Critical infrastructure and Business Critical infrastructure (Option 3), and proactively refreshing all infrastructure (Option 4).

Table 3 – Options evaluated for infrastructure digital resilience

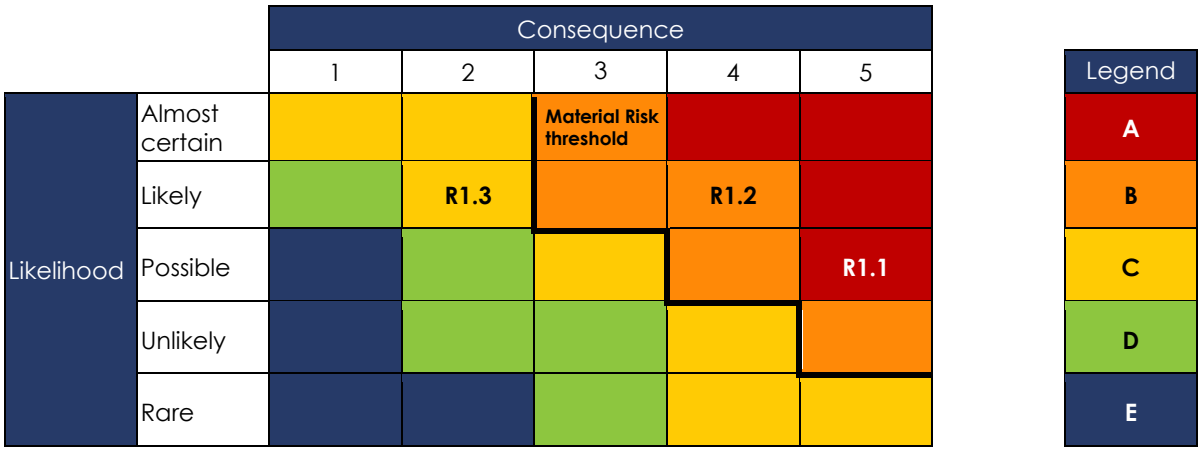
OPTION	SUMMARY
Option 1: No proactive refresh to infrastructure, accept some infrastructure will be operated with no vendor support and reactively manage incidents i.e. a run to failure.	Do not undertake lifecycle refresh of infrastructure or data centre facilities. Reactively manage cyber events or other incidents in-house through operational expenditure directed at mitigating the consequence of the incident, and capital expenditure if the mitigating action requires a refresh or investment following an incident.
Option 2: 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 3: Proactive lifecycle refresh on Mission and Business Critical infrastructure, leveraging vendor extended support arrangement and patch/parts availability. **(Recommended option)**	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 4: 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.

3.2.1. Option 1 – Reactively manage all infrastructure

Under this option, we would not undertake periodic refreshes in line with support timelines and/or expected life of infrastructure. We would expect a higher occurrence of cyber threats, failures and other incidents. This would require reactive support within the business resulting in higher operational expenditure. This would also necessitate reactive capital expenditure on infrastructure, as the result of the run to failure approach, where spares or patches are not available and replacement is only option to avoid a repeat occurrence or address cyber vulnerabilities once known.

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 1.4 and are above AusNet's material risk threshold.

Table 44 - 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 infrastructure 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 infrastructure become inoperable causing significant risk of security intrusion, inability to comply with obligations, and financial infrastructure 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	C

Costs for this option are shown in **Table 5** below. Reactive management of infrastructure in-house, is anticipated to require progressively higher opex due to growth in the support organisation required to provide response to issues and outages. Further capex would still be required for refresh to prevent future occurrence of the incident.

Table 55 - Forecast expenditure for Option 1 ($million real 2025, transmission network allocated costs)

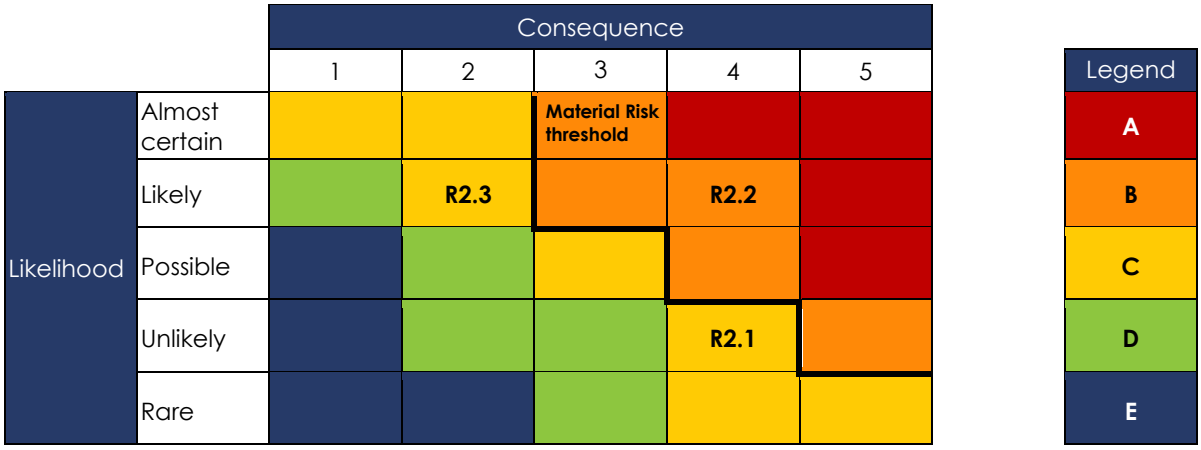
Cost item	RY28	RY29	RY30	RY31	RY32	Total
Capex	$2.97	$2.11	$3.34	$3.56	$2.02	**$14.00**
Opex	$1.81	$1.62	$2.33	$2.71	$1.60	**$10.07**
Total	**$4.78**	**$3.73**	**$5.67**	**$6.27**	**$3.62**	**$24.07**

3.2.2. Option 2 – Proactive refreshes on Mission 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 all Mission Critical infrastructure including data centre facilities, telecommunications, and fire suppression equipment. This reflects the criticality of this infrastructure to supporting mission critical applications maintaining energy security in Victoria. 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 consistent with Option 1 above.

As can be seen from **Table 6** below, the risks are lower than Option 1 for system failures or station events with a reduction in consequence. For example, the SCADA system is less likely to become inoperable, and response time improved. Other risk levels do not vary compared to Option 1, with business wide disruption risk remaining above AusNet's material risk threshold.

Table 667 - 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 infrastructure 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

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

Table 78 9- Forecast expenditure for Option 2 ($million real 2025, transmission network allocated costs)

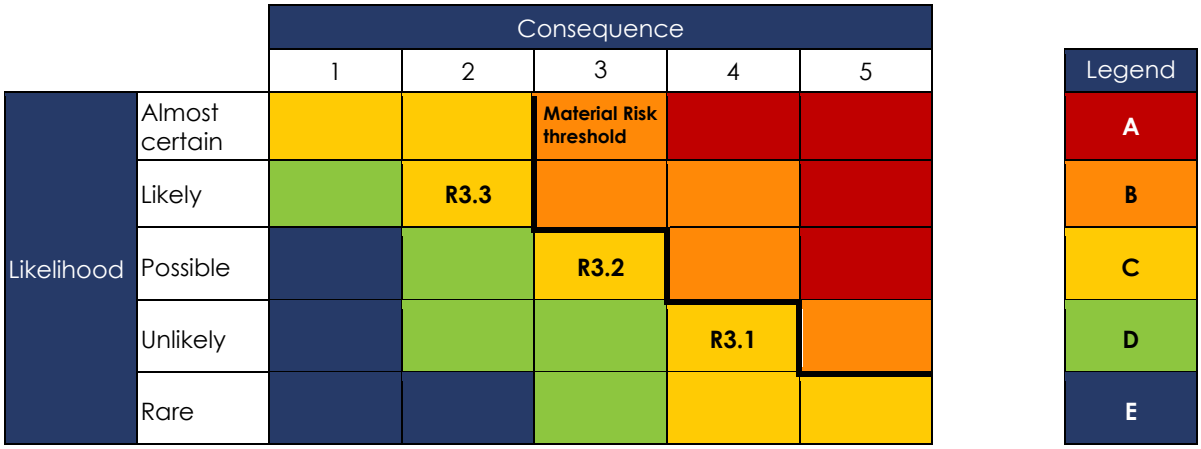
Cost item	RY28	RY29	RY30	RY31	RY32	Total
Capex	$3.10	$2.24	$4.23	$5.10	$2.06	**$16.72**
Opex	$1.64	$1.46	$1.67	$2.30	$1.44	**$8.50**
Total	**$4.74**	**$3.70**	**$5.90**	**$7.40**	**$3.50**	**$25.22**

3.2.3. Option 3 – Proactive lifecycle refreshes on Mission and Business Critical infrastructure

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 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 infrastructure. Business efficiency risks remain unchanged from Section 1.3 inherent risk, with ongoing reactive management.

Table 810 - 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	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 system but opex reduces. The cost of this option includes $0.2 million capex ($real 2025) for reactive user device upgrades when incidents are logged, rather than undertaking scheduled periodic replacement which would cost $1.2 million. 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 11 - Forecast expenditure for Option 3 ($million real 2025, transmission network allocated costs)

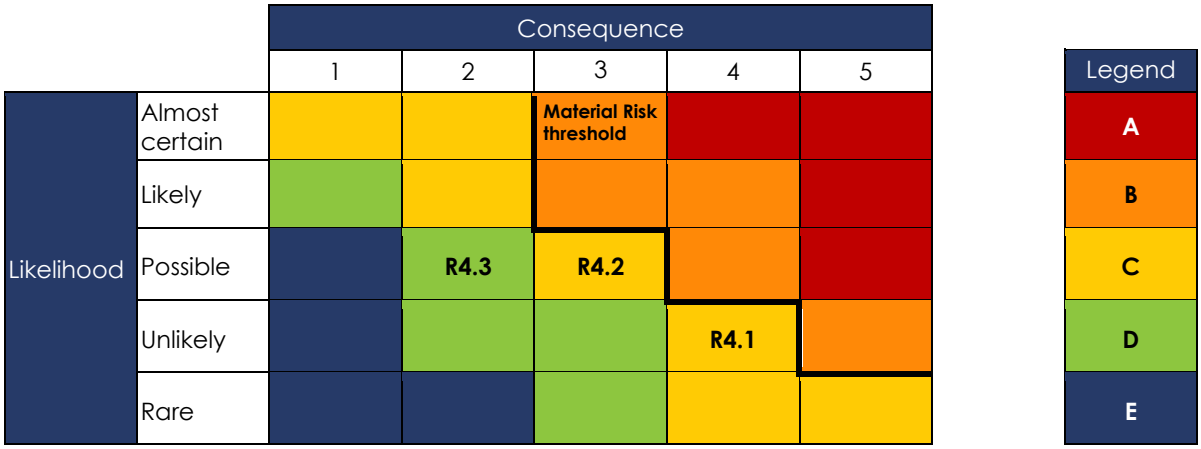
Cost item	RY28	RY29	RY30	RY31	RY32	Total
Capex	$5.60	$4.37	$6.96	$7.76	$4.24	**$28.93**
Opex	$0.07	$0.07	$0.07	$0.07	$0.07	**$0.34**
Total	**$5.67**	**$4.44**	**$7.03**	**$7.83**	**$4.31**	**$29.27**

3.2.4. Option 4 – 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 3. This is reflected in cost difference between Option 3 and Option 4. 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 to 3. This can be seen in **Table 10** where there is lower risk of incidents resulting in in disruption or inefficiency of specific business activities.

Table 10 - Risk assessment of Option 4



	RISK	CONSEQUENCE	LIKELIHOOD	RISK RATING
R4.1	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	Unlikely	C

		dependency outages, and more timely response with vendor support		
R4.2	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
R4.3	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 11 below shows the costs of this option. Capex is higher than Option 1, 2 and 3 as refreshes are required for all infrastructure, but there is a reduction to opex from not having to manage any infrastructure in-house. Further risks to the business are as low as possible including the risks relating to specific business functions.

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

Cost item	RY28	RY29	RY30	RY31	RY32	Total
Capex	$8.75	$7.02	$11.62	$12.38	$6.85	**$46.6**
Opex	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
Total	**$8.75**	**$7.02**	**$11.62**	**$12.38**	**$6.85**	**$46.6**

3.3. Preferred option

Our assessment found that Option 3, proactive refreshes for Mission Critical and Business Critical infrastructure, is the preferred option. This option most cost effectively manages infrastructure digital resilience risks within AusNet's Material Risk threshold as shown below. If maximises the useful life of infrastructure assets by leveraging the vendors' extended support arrangements and replaces assets by the vendor end of extended support date. The marginal risk reduction provided in Option 4 is not commensurate to the increase capex cost required over Option 3.

Criteria	Option 1	Option 2	Option 3	Option 4
Capex ($million, real 2025)	14.0	16.7	28.9	46.6
Opex ($million, real 2025)	10.1	8.5	0.3	0.0
Reduces risks below Material Risk threshold	✗	✗	✓	✓
Preferred option	✗	✗	✓	✗

The costs of this recommended option are $28.93m capex and $0.34m 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 infrastructure 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	$5.60	$4.37	$6.96	$7.76	$4.24	$28.93
Opex	$0.07	$0.07	$0.07	$0.07	$0.07	$0.34
Total	**$5.67**	**$4.44**	**$7.03**	**$7.83**	**$4.31**	**$29.27**

Appendix A – Program cost estimates

Table 13 sets out the cost basis for infrastructure upgrades, 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 – Costings by infrastructure ($ million, real 2025)

INITIATIVES - Digital applications	CAPEX, total RY28-32
Mission Critical systems	
Mission - other infrastructure upgrades	(C-I-C)
Telecommunications Systems hardware	(C-I-C)
Fire suppression	(C-I-C)
Data centre facilities	(C-I-C)
Business Critical systems	
High Security Network	(C-I-C)
Shared Data Centre Infrastructure	(C-I-C)
SCADA Data Historian Infrastructure	(C-I-C)
Business - other infrastructure upgrades	(C-I-C)
System Integration Platforms - HW	(C-I-C)
Physical security digital infrastructure	(C-I-C)
OT Comms Equipment firmware updates	(C-I-C)
Business Operational and Administrative systems	
End user devices (laptops, mobile, peripherals) – *reactive management*	(C-I-C)
TOTAL	(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