Business case: Telecommunications Systems

2025-30 Regulatory Proposal

Supporting document 5.13.2

January 2024

SA Power Networks

Empowering South Australia

Contents

Glossary

Acronym / term	Definition
AER	Australian Energy Regulator
AMP	Asset management plan
ASD	Australian Signals Directorate
BAU	Business as Usual
Capex	Capital expenditure
CIGRE	CIGRE is a global community committed to the collaborative development and sharing of end to end power system expertise
CSF	Cybersecurity Framework
DER	Distributed energy resources
ICT	Information and Communication Technology
LV	Low voltage
MPLS	Multiprotocol Label Switching
NIST	US National Institute of Standards and Technology
NMS	Network Management System
NPV	Net present value
Opex	Operating expenditure
PDH	Plesiochronous Digital Hierarchy
RCP	Regulatory control period
SDH	Synchronous Digital Hierarchy
TNC	Telecommunications Network Control

1 About this document

1.1 Purpose

This document provides a business case to support forecast expenditure for the 2025-30 regulatory control period (**RCP**) on the program of Telecommunications Systems, which comprises of Telecommunications Network Control (**TNC**) Management Systems, Operational Telephone Network and Business Telephone Network as input to our overall network asset replacement expenditure.

1.2 Expenditure category

- Non-network capital expenditure (**capex**): other non-network

1.3 Related documents

Table 1: Related documents

Ref	Title	Author	Version / date
[1]	AP 3.3.07 Telephony	SA Power Networks	2025-2030 / May 2023
[2]	AP 3.3.08 TNC Systems	SA Power Networks	2025-2030 / May 2023

2 Executive summary

This business case recommends **$5.97 million**[1] in recurrent capex to support the ongoing refresh of the telecommunications systems in line with previous RCPs to:

- support the current capacity to monitor and manage our telecommunication networks;
- support the monitoring and management of changing telecommunication technologies and their use within these networks; and
- support the continued operations of our operational and business telephone networks.

We have been investing in our Network Management Systems (**NMS**) and increasing their capabilities and functionality to provide ongoing, contemporary system management. As components of the communications networks reach end of life they are reviewed, and where required modernised to maintain and improve functionality.

The key drivers for the progressive development of our systems over the last five years have been:

- increasing use of 4G services for midline distribution equipment and some substation services where no other communications network is available;
- continuing migration from end-of-life Synchronous Digital Hierarchy (**SDH**) and Plesiochronous Digital Hierarchy (**PDH**) based communications equipment to Multiprotocol Label Switching (**MPLS**) equipment changing our monitoring and management capability needs;
- continuing migration from end-of-life Pilot Cable infrastructure to fibre optical network; and
- continuing migration from unsupported radio links to fully supported and manageable radio links.

The operational telephone network forms part of the secure voice communications system that supports communications from our control centers to substations across our distribution network. There are ongoing replacement and refresh activities for this network to continue to provide secure and reliable voice communications supporting a safe operating environment for our people and safe and reliable operation of the distribution network.

This business case recommends a continuation of the current programs to maintain the current capabilities across both the NMS and telephone systems. The 2025-30 RCP forecast of $5.97 million recurrent expenditure for the program represents an increase of $1.46 million compared to the 2020-25 period and is a direct result of technology developments, network evolution and systems supportability.

The net present value (**NPV**) over the 5-year period is **-$5.39m** and the overall residual risk rating is **Medium**.

Another option considered was to *invest at elevated levels of expenditure into interim legacy technology*. While this level of investment does manage some risk (compared to no investment), it will result in increasing costs over time as impending changes in technology become unavoidable. Delays to technology migration can negatively impact safety, network performance and service delivery.

The preferred option was selected because it:

- maintains our existing systems and services at the current acceptable levels of risk;
- allows us to respond to the changes in telecommunications technology and to ensure network performance levels can be maintained in a rapidly evolving environment; and
- retains the capabilities created when these systems were implemented.

[1] Unless otherwise specified, all financial figures in this business case are in real June 2022 dollars.

3 Background

3.1 The scope of this business case

This business case is for recurrent telecommunications systems expenditure to enable continuous day to day operation and monitoring of our distribution and telecommunications networks and continue to provide critical operation and business telephony.

3.2 Our performance to date

Our spend profile in the 2020-25 RCP is in line with the associated asset plans (AP 3.3.08 -TNC Management Systems and AP 3.3.07 – Business and Operational Telephony).

The primary focus for telecommunications systems is the NMS platform that monitors all critical telecommunications nodes. The development of new generation platforms delivering efficiency gains via new and improved NMS functions is the driver for system upgrades and replacements.

Changes to telephony and TNC systems driven by external influences have required variations to the asset plans to compensate for out of schedule expenditure.

Table 2: $'000, June 2022[2]

Program	Allowance	Actuals / Forecast
TNC Systems AP 3.3.08	2,853	4,059
Telephony AP 3.3.07	2,230	451
Total	**5,084**	**4,510**

3.3 Drivers for change

In the 2025-30 RCP, we are proposing a business-as-usual approach based on our historic expenditure to upgrade our technology, systems and service contracts. For further information refer to our asset plans AP 3.3.08 - Telecommunications Network Control Management System and AP 3.3.07 - Operational Telephony which are available on request.

3.4 Industry practice

We regularly consult and collaborate with industry bodies, peers, and partners such as CIGRE, Electranet, and system vendors to guide the telecommunications group when developing asset plans and relevant business cases. For example, SA Power Networks and Electranet have been independently reviewing NMS systems and have developed similar system requirements to investigate potential replacement systems. This consultation informed and validated the reasoning in the asset plans that support this business case by providing consistency and alignment with peer organisations. Maintaining consistency within the electricity industry enhances capability, resource access and collaboration opportunities, which in turn helps us ensure efficiency of our costs and prudency of our ongoing technology investments.

[2] Totals presented in tables throughout this document may not exactly match the sums of individual figures due to rounding.

4 The identified need

We forecast that in at least the next two regulatory control periods that there will be an increasing volume of work on our distribution network, as we need to increase network capacity to respond to increasing demand for service (load and export), and the need to retire and replace assets due to their age and deteriorating condition. Meeting and managing demand for service, complying with regulatory requirements and otherwise maintaining reliability, safety, security and quality of supply will in coming years require increases in our overall network expenditure relative to our current expenditure levels.

This business case responds to this challenge, by seeking to explore opportunities to minimise the costs of delivering this increased volume of work in coming years. Through our experience in operating and maintaining TNC and telephone systems we have seen the potential for technology progression to drive improvements in systems and asset management. This business case identifies the reasons for investing in these systems and processes over the 2025-30 RCP for a net benefit to consumers.

This business case also seeks to address the concerns of our customers as expressed through our engagement program, that we invest to continue improving our monitoring, control and asset management practices and processes to ensure that we are making use of new technologies to drive reductions in the cost of delivering network activities in the field. This was an explicit recommendation of our customers, as reflected in the recommendations of the People's Panel.

Further to this, the Australian Government passed legislation in 2018 for the Security of Critical Infrastructure which imposes additional cyber security requirements on identified industry sectors.

On 2 April 2022, the Security of Critical Infrastructure Act 2018 was amended, introducing a new enhanced cyber security obligations framework for systems of national significance —Australia's most important critical infrastructure assets.

As part of this legislation the Secretary for Home Affairs can declare an entity to be a Systems of National Significance and as part of this declaration the entity may then be subject to the enhanced cyber security framework and detailed vulnerability assessments.

As part of our cyber security SA Power Networks continues adopting the Australian Signals Directorate (**ASD**) Essential Eight recommendations in addition to elements of the cybersecurity standards developed by the US National Institute of Standards and Technology (**NIST**) Cybersecurity Framework (**CSF**).

The Essential 8 recommendations require businesses to ensure that all critical software systems are maintained on supported versions and are regularly patched.
The NIST Cybersecurity Framework is a global standard for cybersecurity and protection of critical infrastructure. It has five core objectives:

- Identify: assessing the threats and risks to systems and understand the vulnerabilities
- Protect: defending systems from attack with best practice approaches
- Detect: having tools and protocols in place to spot when a breach has happened
- Respond: reacting quickly using automated safeguards to contain the breach and have protocols in place to mobilise resources
- Recover: having plans in place to handle the aftermath, communicate the outcomes and review the learnings.

To meet these objectives and to pass vulnerability assessments our software systems must be maintained on supported versions. Unsupported and unpatched software does not meet the requirements for protection and may reduce the ability for a business to detect and respond to a cyber-attack.

5 Comparison of options

5.1 The options considered

Table 3: Summary of options considered

Option	Description
Option 0 – Maintain current functions and capabilities	Continuation of the current programs to maintain functions and capabilities across both Telecommunications Systems and Telephone Systems consistent with the 2020 -2025 RCP. This option is proposed to address technology developments, network enhancement and systems supportability including: • Business as Usual (BAU) – risk based management of Telecommunications Systems and telephony to maintain OT services and functions required within 2025-2030 regulatory control period • Ongoing investment in technology rollout consistent with the 2020-2025 RCP • Manage EOL (end of life) Alcatel SDH nodes and NMS 1350 system until MPLS services are fully provisioned circa 2030 • Manage EOL Nokia PDH equipment and NMS systems until MPLS services are fully provisioned circa 2030 • Manage unsupported radio link systems until supported radio link equipment is deployed circa 2030
Alternative options	
Option 1 – Increase in investment on interim legacy systems	Increased investment to upgrade and replace unsupported systems with interim legacy systems during the 2025-2030 RCP, delaying some technology migration in to the 2030-2035 RCP. This option assigns capital investment into short lived legacy assets but does not offset the mid to near term replacement of these assets: • Alcatel SDH node firmware upgraded to supported versions. • Alcatel SDH node hardware replaced with supported versions. • Alcatel NMS 1350 system replaced with current supported versions. • Nokia PDH nodes and management systems replaced with alternate PDH hardware from alternate vendors.

5.2 Options investigated but deemed non-credible

We considered an option to reduce investment in current systems and technology deployment with risk-based management of legacy systems. This option was deemed non-credible for the following reasons:

- Loss of value in previously deployed technology development (2015-20 and 2020-25 RCP)
- Limited options and lifespan for legacy risk management
- Increased cyber risks with hybrid deployment
- Increased costs for long term maintenance of legacy equipment/management skill sets
- Minimal reduction in total (capex + opex) investment over Option 0, due to ongoing maintenance over new and old technologies

5.3 Analysis summary and recommended option

5.3.1 Options assessment results

Table 4: Costs, benefits, and risks of alternative options relative to the base case over the 5-year period, $m, Dec 2022 real.

Option	Costs		Benefits[3]		NPV[4]	Risk Level[5]	Ranking
	Capex[6]	Opex[7]	Capex	Opex			
Option 0 - Maintain current functions and capabilities	5.97	0.00	0.00	0.00	-5.39	Medium	1
Option 1 - Increased investment on interim legacy systems	6.60	0.00	0.00	0.00	-6.01	High	2

5.3.2 Recommended option

Option 0 (base case) is recommended to ensure the continuation of the current programs to maintain functions and capabilities across both Telecommunications Systems and Telephone Systems consistent with the 2020 -25 RCP. This option is proposed to address technology developments, network enhancement and systems supportability.

The 2025-30 RCP forecast of $5.97 million recurrent expenditure for the program represents an increase of $1.46 million compared to the 2020-25 period.

[3] Represents the total capital and operating benefits, including any quantified risk reductions compared to the risk of Option 0 (base case), over 5-year cash flow period from 1 July 2025 to 30 June 2030 expected across the organisation as a result of implementing the proposed option.
[4] Net present value (NPV) of the proposal over 5-year cash flow period from 1 July 2025 to 30 June 2030, based on discount rate of 4.05%.
[5] The overall risk level for each option after the proposed program is implemented. Refer to Appendix B– risk assessment for details.
[6] Represents the total capex associated with the proposed option over the 5-year cash flow period from 1 July 2025 to 30 June 2030.
[7] Represents the total opex increase associated with the proposed option above the current level of opex, over the 5-year cash flow period from 1 July 2025 to 30 June 2030.

5.4 Option 0: Maintain current functions and capabilities

5.4.1 Description

Continuation of the current programs to maintain functions and capabilities across both Telecommunications Systems and Telephone Systems consistent with the 2020-25 RCP.
This option will require some unsupported systems to be maintained in the short term (5yrs) while technology migration is undertaken. The risks associated with the unsupported systems are understood, mitigated, and managed.

5.4.2 Costs

The Option 0 forecast includes $5.97 million in capital expenditure, as shown in Table 5.

Table 5: Option 0 Costs by Cost Type ($m June 2022 Real)

Cost Type	2025-26	2026-27	2027-28	2028-29	2029-30	Total 2025 - 30
Capex	0.64	2.16	0.91	0.43	1.83	**5.97**
Opex	0.00	0.00	0.00	0.00	0.00	**0.00**
TOTAL COST	**0.64**	**2.16**	**0.91**	**0.43**	**1.83**	**5.97**

5.4.3 Risks

Table 6: Risk assessment summary

Risk consequence category	Residual risk level[8]
Safety - Harm to a worker, contractor, or member of the public	**Low**
Network - Failure to transport electricity from source to load	**Low**
Technology & Data Capability – Disruption of access, or use of systems	**Medium**
Customers - Failure to deliver on customer expectations	**Medium**
Overall risk level	**Medium**

5.4.4 Quantified benefits

There are no quantified benefits in this business case.

5.4.5 Unquantified benefits

- Benefits that can be quantified:
  - Continuation of network monitoring and management capability to provide operational safety, continuity, and security
  - Increased flexibility and functionality of management systems to provide fast, effective, and efficient response to network faults and alerts
  - Increased visibility of network asset data such as historical and statistical analysis
  - Ability to perform predictive analysis to advance inspection and maintenance programs

[8] The level of risk post current controls (ie after considering what we currently do to mitigate the risk).

  - Ability to share network information with field operations in a safe and secure manner
  - Reduce duplication of system information to reduce data and record keeping errors
  - Ability to leverage system intelligence and automation for efficiency and performance
  - Longer term reduction in legacy technology and reliance on outdated specialist skills sets
  - Portability and availability of technical skills for staff and contractors
  - Consistency of technology with other industry entities
  - Appealing technology and career path for staff and graduate retention
- Benefits that cannot be quantified:
  - Longer-term reduction in legacy technology and reliance on outdated specialist skills sets
  - Portability and availability of technical skills for staff and contractors
  - Consistency of technology with other industry entities
  - Appealing technology and career path for staff and graduate retention

5.5 Option 1: Increased investment on interim legacy systems

5.5.1 Description

Option 1 presents an increased investment to upgrade and replace unsupported systems, such as SDH and PDH, with interim legacy systems during the 2025-30 RCP, delaying some technology migration in to the 2030-35 RCP.

This option would replace unsupported legacy technology with supported legacy technology, where available, or would upgrade unsupported systems to be in support for a short-term benefit while the technology transition progresses. The increased investment to bring legacy technology into support would reduce the investment in new technology transition, thus extending the time required to divest systems of legacy technology. While some legacy systems are still available and supported, it does increase the risks of labor skill set capability and staff shortages in managing the legacy technology.

While legacy systems are still currently available, industry trends are clearly indicating these systems have minimal long-term viability and skillsets to maintain such legacy systems are already a significant risk factor.

5.5.2 Costs

The Option 1 forecast includes $6.60 million in capital expenditure, as shown in Table 7.

Table 7: Option 1 Costs by Cost Type ($m June 2022 Real)

Cost Type	2025-26	2026-27	2027-28	2028-29	2029-30	Total 2025 - 30
Capex	1.20	2.25	1.05	0.40	1.70	**6.60**
Opex	0.00	0.00	0.00	0.00	0.00	**0.00**
TOTAL COST	**1.20**	**2.25**	**1.05**	**0.40**	**1.70**	**6.60**

5.5.3 Risks

Table 8: Risk assessment summary

Risk consequence category	Residual risk level[9]
Safety - Harm to a worker, contractor, or member of the public	Low
Network - Failure to transport electricity from source to load	Low
Technology & Data Capability – Disruption of access, or use of systems	High
Customers - Failure to deliver on customer expectations	High
Overall risk level	High

5.5.4 Quantified benefits

There are no quantified benefits associated with this option.

5.5.5 Unquantified benefits

- Legacy systems will have manufacturer support for the duration of the technology migration.

[9] The level of risk post current controls (ie after considering what we currently do to mitigate the risk).

6 Deliverability of recommended option

The proposed option is a continuation of existing works programs as delivered in the 2015-20 and 2020-25 RCPs within our Network Management – Operational Technology and Data business unit.

Our ability to resource the program of work proposed in this business case has been demonstrated over the last two RCPs by successfully completing similar programs of work.

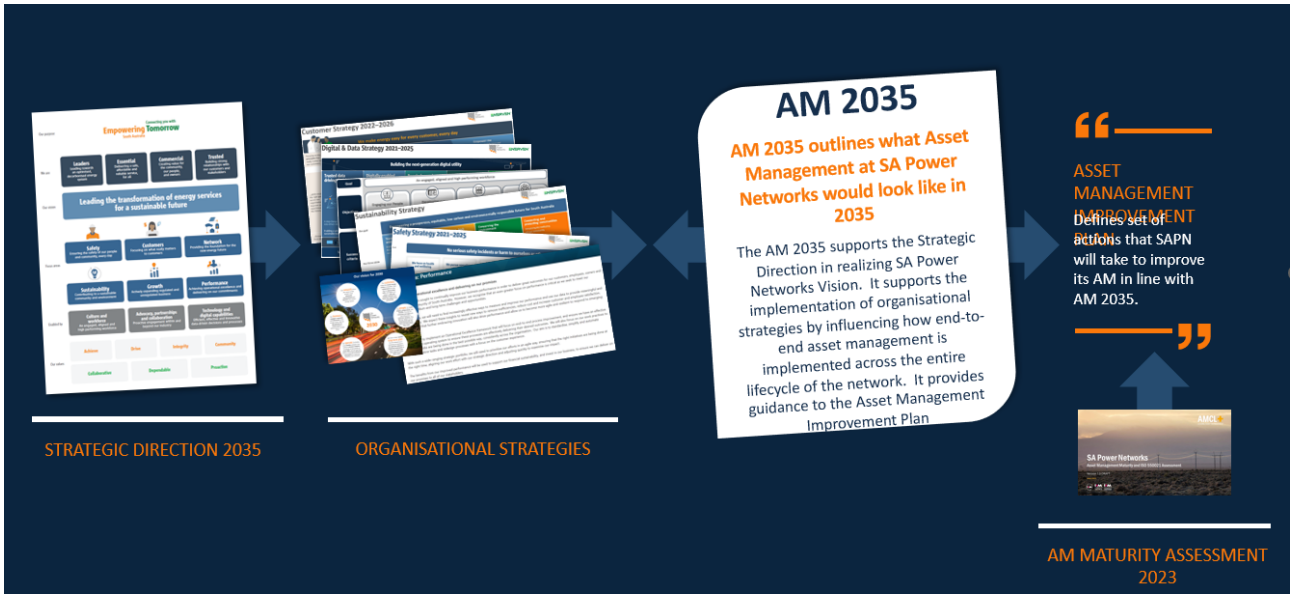
7 How the recommended option aligns with our engagement

7.1 Alignment to customer expectations

Customers expect that we will maintain our existing levels of service and risk. This investment meets those requirements in a cost-effective manner. Secure, reliable and supportable infrastructure enable SA Power Networks to achieve components of these themes by ensuring our workforce can access data, respond to jobs, and manage the network to expectations, and can do this within specified key performance requirements.

7.2 Alignment with our vision and strategy

Figure 1: Asset Management Vision development

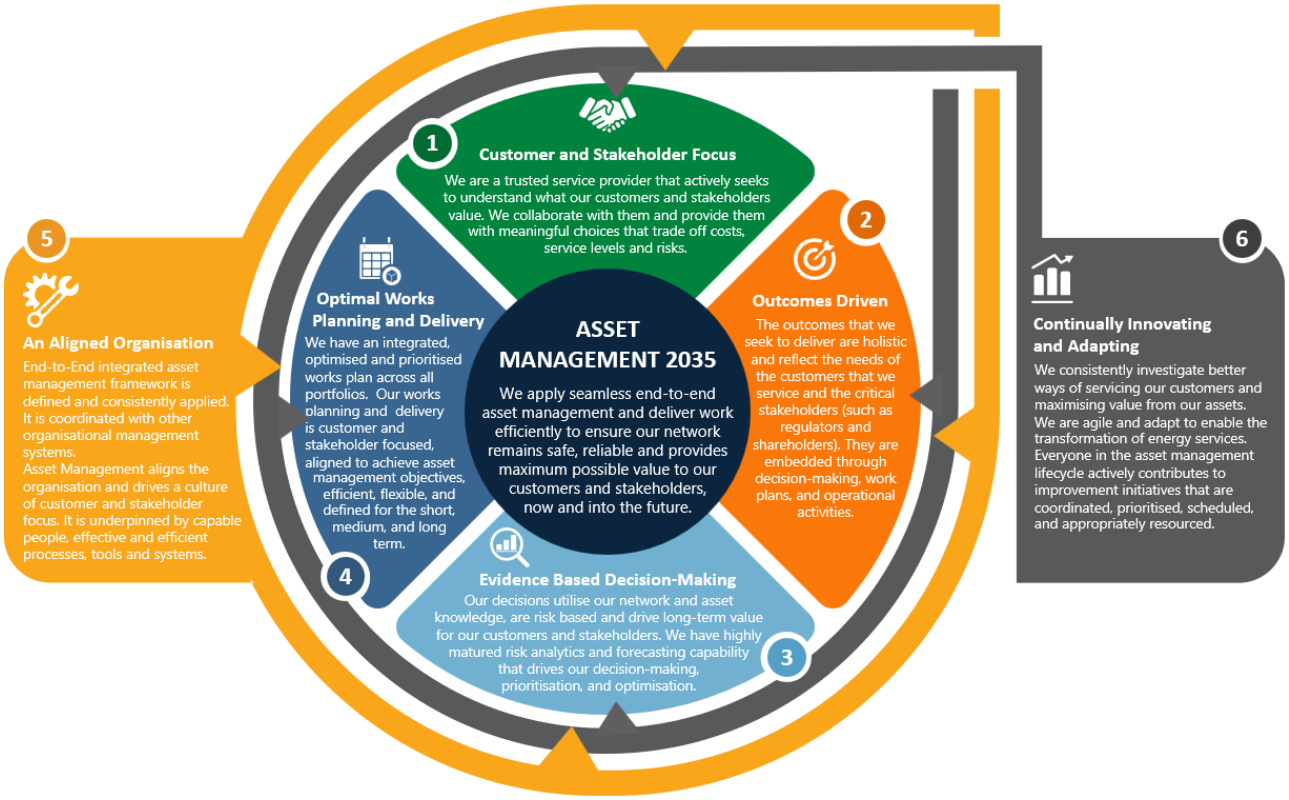


Our Asset Management is informed by our recently developed Asset Management 2035 Vision aligned with our corporate Strategic Directions 2035 and other organisational strategies.

First, we **focus** on what our **customers and stakeholders** value. The **outcome**s we seek to deliver through our assets reflect the needs of our customers and stakeholders. We combine this with **evidence-based decision making** to inform our response and develop **optimal works planning and delivery**. We achieve this through **an aligned organisation** and by **continually innovating and adapting** how we do things by empowering our people, investing in our asset management system, and piloting and trialling new technologies and concepts.

Our Asset Management Vision guides our Assets Management Transformation program.

Figure 2: SA Power Networks Asset Management Vision



8 Reasonableness of cost and benefit estimates

Cost estimates are derived from historical data from two RCPs from 2015 to 2025 and associated network history.

The proposed option is a recurrent expenditure, business as usual model with risk-based management of assets, and incremental safety, system continuity, security, and performance improvements as objectives. Asset management plans (AMP's) are maintained to guide the replacement and expenditure decisions based on the given technology type.

AMP's list the known condition, equipment support status and risks associated with equipment or technology class. AMP's are updated based on manufacturer information, inspection programs and resultant feedback, technology progression and business requirements.

Each AMP covers a technology class or specific type of equipment.

9 Reasonableness of input assumptions

Input assumptions are derived from historical data from two RCPs from 2015 to 2025 and associated network history. The proposed option is a recurrent expenditure, business as usual model with risk-based management of assets, and incremental safety, system continuity, security, and performance improvements as objectives.

A. Appendix A – cost models

Cost estimation and NPV analysis template:

2025 - 30 Reset - Project-Program Template with instructions Opt 0 Base Case
2025 - 30 Reset - Project-Program Template with instructions Opt 1

B. Appendix B - Risk assessment

The risk assessment shown indicates Option 0 to have a lower rating than Option 1 even though Option 1 has the higher capital expenditure. This is due to Option 1 representing a delay of several years for the full transition to newer technology types that have inherent improvements in encryption, redundancy and supportability, and importantly, the two systems are not directly interoperable.

While Option 1 does represent deploying 'new' legacy technology, the deployment must be interoperable with the existing legacy systems that have limited or restricted capability in the areas mentioned above, in addition mitigation of these aspects is also compromised due to interoperability, that is, connecting the new to the old can compromise the newer system.

The increased risk of operating 'new' legacy systems is reflected in the risk matrix as the same consequence (same issues), but higher likelihood (longer duration of exposure).

				Current risk (Option 0)			Residual risk (Option 1)		
ID	**Risk scenario**	**Consequence description**	**Consequence category**	**Consequence**	**Likelihood**	**Risk Level**	**Consequence**	**Likelihood**	**Risk Level**
1	Risk scenario 1 Loss of network visibility and/or control	Impact on operator safety	**Safety**	3	1	Low	3	1	4 Low
		Impact on system continuity	**Network**	3	2	Low	3	2	5 Low
		Impact on system security	**Technology and Data Capabilities**	4	2	Medium	4	2	Medium
2	Risk scenario 2 Degraded voice communications	Impact on operator safety	**Safety**	3	1	Low	3	1	4 Low
		Impact on system continuity	**Network**	3	1	Low	3	1	4 Low
3	Risk scenario 3 Disclosure, loss or destruction of OT data	Impact on operator safety	**Safety**	1	2	Minimal	1	3	Low
		Impact on system continuity	**Network**	1	2	Minimal	1	3	Low
		Impact on system security	**Technology and Data Capabilities**	4	2	Medium	4	3	High
		Impact on customer expectations	**Customers**	4	2	Medium	4	3	High
			Overall Risk Level[10]			Medium			High

[10] For each option, the overall risk level is the highest of the individual risk levels.