Options Evaluation Report (OER)

Infrastructure and Network

Approvals

Author	Marnie Williams	IT Strategy Business Partner
Endorsed	Delan Naidu	IT Technology Domain Manager
	Andrew Dome	IT Digital Operations and Experience Manager
Approved	Russell Morris	Chief Information Officer
Date submitted for approval	15 November 2021	

Change history

Revision	Date	Amendment
Version 0.2	8 Jul 21	Updated the OER to reflect the feedback from Andrew Dome
Version 0.8	31 Aug 21	Updated the OER to reflect the feedback from HoustonKemp and copywriter
Version 0.9	31 Aug 21	Updated the outage calculation
Version 1.0	15 Nov 21	Updated for Nov 15 submission to reg team

Executive summary

This Options Evaluation Report (OER) assesses the options for maintaining and refreshing the assets of our Corporate Data Network (CDN), which are obsolescent and increasingly unreliable.

The period 2018 to 2023 saw minimal investment in CDN assets and infrastructure as ICT expenditure was directed towards more critical areas. The resulting increased risk of business outages needs to be remediated in the next regulatory period. [redacted]. Maintaining aging technology is expensive and runs the increasing risk of security threats, non-compliance and hardware failure.

[redacted]

Modernising our infrastructure and CDN assets will allow us to adopt technology that provides flexibility in the workplace, such as Desktop as a Service (DaaS), allowing us to scale, and be adaptive and responsive to future business needs, including future energy transition requirements.

This OER considers two options:

1. A Base Case to refresh infrastructure and CDN assets using a risk-based approach. We believe we can extend asset lives beyond those recommended by vendors without a material increase in outage risk. The Base Case would also involve moving certain infrastructure to the cloud, in line with our current transition to a hybrid (mix of on-premise and cloud) environment.

2. Option 1 would be similar to the Base Case but would instead refresh infrastructure and CDN assets according to vendor's recommended asset life cycle. This option would also modernise our CDN network by transitioning to a next generation network.

The Base Case would provide us with a security and reliable network where the risk of outage is considered to be low. Although Option 1 would mitigate some additional security and technology vulnerabilities, we do not consider this to be a prudent investment considering the additional cost it involves. As such, our preferred option for this OER is the Base Case.

Table 1: Evaluated options

Option	Description	Direct Capital Cost ($m)	Network & Corporate Overheads Cost ($m)	Total Capital Cost ($m)	Net Present Value (NPV) ($m)	Rank
Base Case	> Refresh infrastructure and CDN assets to supportable versions to maintain a continuous service > Introduce a hybrid environment that combines on-premise and cloud-based platforms > Provide a scalable modern network that can meet critical business needs such as work-from-anywhere and future energy transition requirements	[redacted]	[redacted]	$19.28	1.55	1

Option	Description	Direct Capital Cost ($m)	Network & Corporate Overheads Cost ($m)	Total Capital Cost ($m)	Net Present Value (NPV) ($m)	Rank
Option 1	Base Case + > Refresh CDN assets that have been categorised as important. > Modernise our CDN by transitioning to a next generation network.	[redacted]	[redacted]	$24.14	-$2.44	2

The proposed capital expenditure for the preferred option, Base Case, is summarised below:

IT Capex $M	FY24	FY25	FY26	FY27	FY28	TOTAL
Recurrent costs	$5.12	$3.84	$4.80	$5.27	$0.25	$19.28
Non-recurrent costs	0	0	0	0	0	0
TOTAL	***$5.12***	***$3.84***	***$4.80***	***$5.27***	***$0.25***	***$19.28***

The numbers in this OER represent the total cost of ownership for an asset consistent with past submissions. There has been a change in accounting practices associated with IFRS[1] that has come in place. The proposed capital expenditure for preferred option in this OER shown with IFRS impact is below

IT Capex IFRS $M	FY24	FY25	FY26	FY27	FY28	TOTAL
Recurrent costs	$5.12	$3.84	$4.80	$5.27	$0.25	$19.28
Non-recurrent costs	0	0	0	0	0	0
TOTAL	***$5.12***	***$3.84***	***$4.80***	***$5.27***	***$0.25***	***$19.28***

*No expected change for this OER as the forecast is for like for like replacement solutions. No Software as a Service (SaaS) type solutions are proposed for this OER.

[1] International Financial Reporting Standards Foundation (IFRS Foundation) ruling means that in the 2023-28 period we will expense costs for configuration or customisation in cloud computing arrangements, whereas in the 2018-23 regulatory period these costs were treated as capex.

1. Need/Opportunity

1.1 Background

For our staff to operate the transmission network and serve our customers, we depend on an efficient internal data network and associated IT devices such as routers, servers and data storage devices, collectively known as the Corporate Data Network (CDN). The CDN enables staff across our offices, depots and other remote sites to access: corporate information, our intranet and internet, and internal files, including work plans and incident reports; essential digital tools, such as Microsoft Office and Outlook; and communication and collaboration facilities, such as video conferencing.

Currently, the assets of CDN [redacted] – see the Appendix for a summary of CDN assets and their end of life timing – [redacted]. Like all technology, the equipment that makes up the CDN requires refreshing at end of life to prevent: asset failure as equipment ages and becomes less reliable; and obsolescence as technology becomes incompatible with new equipment or software or performance levels no longer meet business requirements.

If a device fails, the resulting CDN outage prevents our staff from gaining access to the data and tools essential to do their jobs. [redacted]

Similarly, a network outage leaves field staff no longer able to access maintenance work plans or incident reports, preventing them from completing tasks in a safe and efficient manner.

1.1.1 Why is this important?

To ensure the continuing interoperability of the CDN and the software that runs across it, equipment needs to be gradually replaced and other parts of the underlying infrastructure require regular updates.

[redacted]

As a result of failing to maintain infrastructure and the CDN, the business will inevitably suffer a greater number of outages as assets will fail before being replaced. [redacted]

1.1.2 Strategic move to the cloud

Modern CDN infrastructure and assets are also critical to support our cloud strategy. In the period 2023 to 2028, we will continue to move particular applications into the cloud to improve the efficiency of our operations and leverage the latest software updates that are increasingly only being provided as a cloud service.

Moving critical services to the Cloud improves uptime and scalability. Uptime is improved because the infrastructure the service is hosted on, rather than being locally hosted in our data centres, is provided by large-scale vendors, including Microsoft (Azure) and Amazon (AWS). These vendors have the necessary scale, employees, hardware and funding to meet availability times of around 99.9%. With vendors' teams managing service maintenance and upgrades, over time, the operational costs for Cloud services will be lower than for on-premise solutions.

Cloud-hosted services can also be scaled quickly to accommodate rapidly changing workplace needs. An upgrade of a remote working solution like VPN can be activated within hours for a Cloud hosted service. Whereas a similar exercise on an on-premise service could take weeks to implement given the requirement to procure hardware, build and configure, test, and deploy into Production. A scalable service in a Cloud platform enables our employees

to consume services almost instantly, allowing them to get on with their work without having to wait for IT to implement an upgrade over a number of weeks or months.

As we move more applications to the cloud to take advantage of these benefits, CDN infrastructure and assets will need to adapt to a hybrid landscape so we can operate the combined on-premise and cloud-based assets in the most efficient and secure manner.

1.2 Business Drivers

The main business drivers for changes to our Infrastructure and CDN are to:

- Maximise service continuity, minimise business disruption and control maintenance costs by replacing end of life assets based on the IT Asset Management Plan/Information Technology Renewal and Maintenance Strategy[2], which is designed for optimum and cost-effective performance
- Improve the user experience with communication tools, such as video conferencing, by providing a quality and reliable IT service
- Improve the security profile of CDN assets, such as firewalls, that control internal to external traffic to prevent intrusion
- Ensure we can continue to meet compliance, security and safety obligations by having integrity in our systems, security in our data and the ability to report information accurately to our partners, the government and consumers
- Ensure our infrastructure and CDN landscape progressively transitions to modern platforms, such as the cloud.

1.3 Risk Drivers

This program aims to address the following risk:

- **Worker Health & Safety:** Our infrastructure and CDN directly support the health and safety of the community and staff. If infrastructure and the CDN are unavailable or interrupted, information will not be available to staff, including those in the field, preventing people from performing their daily activities. For example, a CDN outage could prevent staff from being able to access incident reports about a construction site, potentially creating negative safety outcomes for staff and the wider community.
- **Reputation:** Service and safety failures due to unavailable data or network services have the potential to cause stakeholder dissatisfaction and adverse media coverage for both TransGrid and the broader energy sector.

  Compliance: Refreshing and maintaining infrastructure and the CDN is essential for these assets to remain current and align with our security guidelines. The security vulnerabilities of aging technology create the increasing risk of unauthorised access, potential interruptions and data loss.
- **Reliability**: The risk of infrastructure and CDN equipment failure increases over time as the hardware reaches its end of useful asset life defined by the vendor. Extending the life of infrastructure and CDN equipment increases the risk of disruptions, which will impact business services that maintain a reliable network and interact with consumers.
- **Finance:** Scheduled work delays, lengthy disrupting and management time required to remediate and respond to the consequences of outages all cost at an escalating cost. Also, as infrastructure and CDN equipment ages the vendor increases the maintenance support costs.
- **People/IR:** Relying on staff with specific skills to maintain aging infrastructure and the CDN introduces key-person risk. The availability of this skill set in the market is diminishing as personnel upskill themselves in modern technologies.
- **Environment:** N/A.

[2] Reference: *Information Technology Renewal and Maintenance Strategy*

2. Related Needs/Opportunities

The subject of this OER is aligned with the following investment opportunities:

ICT Programs/OERs	Related to this program	Relationship commentary
Cyber Security	High – functional	Provides the security guidelines that infrastructure and CDN vendors must follow when refreshing assets covered by this OER.
Data and Decisioning	High – functional	Determines the data guidelines that infrastructure and CDN vendors must follow when refreshing assets covered by this OER.
Employee Enablement	High – functional	Encompasses the end user devices with which the CDN equipment covered by this OER needs to remain compatible and support with adequate performance for increased digital traffic. The refresh covered by this OER will support the introduction of Microsoft's Teams communication capability and the decommissioning of Cisco's Webex.
Application Maintenance	High – functional	Includes changes in the location of business applications as they are upgraded, which will be supported by the recommendations of this OER.
Bespoke Applications	High – functional	Includes changes in the location of bespoke applications, as they are maintained, which will be supported by the recommendations of this OER.
Operational Evolution	High – functional	Includes plans to move our project and portfolio management application (PPM) and automate a number of processes by leveraging cloud-based platforms. These changes will be supported the recommendations of this OER.

3. Options

3.1 Base case – Refresh infrastructure and CDN assets to maintain a continuous service

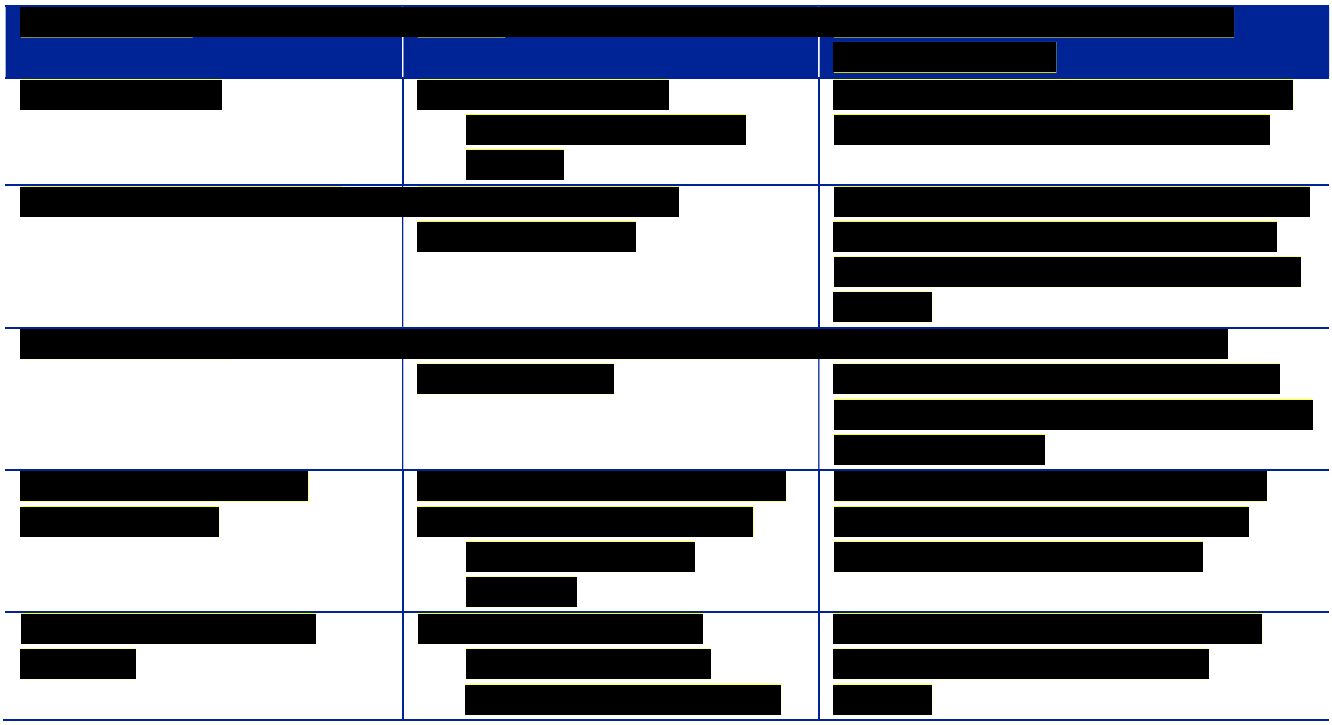
The Base Case proposes refreshing the existing infrastructure and CDN assets to maintain a continuous service. This approach will remove obsolescent infrastructure and CDN assets, mitigate security and technology vulnerabilities and enable us to integrate new communication tools, such as Microsoft's Teams, into the IT landscape.

The Base Case will modernise our technology platforms and support a hybrid landscape that will enable us to provide work from anywhere services to staff and allow us to scale services to meet future business needs. We will also migrate at least 10 applications to cloud-based platforms, enabling us to provide better services to consumers.

[redacted]

To mitigate this risk, we must maintain our CDN assets to an appropriate level. We propose doing this using a risk-based approach, where we balance the cost of refreshing infrastructure with the risk of its failure. Under this approach, we believe we can extend asset lives beyond those recommended by the manufacturer without a corresponding increase in the risk of outage.

[redacted]



This Base Case intends on refreshing the current infrastructure and CDN capability to meet future demand. This is an effective and practical approach, which supports our growth and energy transition needs.

3.1.1 Financial summary

The total IT capital expenditure for the Base Case is estimated to be **$19.28M** spread across the five-year regulatory period as shown below:

Table 2: Financial summary - Base Case

IT Capex $m	FY24	FY25	FY26	FY27	FY28	TOTAL
Recurrent costs	$5.12	$3.84	$4.80	$5.27	$0.25	$19.28
Non-recurrent costs	0	0	0	0	0	0
TOTAL	***$5.12***	***$3.84***	***$4.80***	***$5.27***	***$0.25***	***$19.28***

The costs are based on previous hardware and software replacements and the associated labour required to deliver the service.

Table 3: Financial summary - Base Case

IT Opex $m	FY24	FY25	FY26	FY27	FY28	TOTAL
Recurrent costs	$0.14	$0.14	$0.14	$0.14	$0.14	$0.70
Non-recurrent costs	0	0	0	0	0	0
TOTAL	***$0.14***	***$0.14***	***$0.14***	***$0.14***	***$0.14***	***$0.70***

3.1.1.1 Non-quantifiable benefits

In addition, the Base Case option will:

- Provide a platform that is supported by vendors and scalable to meet our needs
- Ensure the appropriate staffing levels and skillsets to deliver continued service to the business and consumers
- Provide a modernised platform that enables staff to work from anywhere

- Remediate the risks associated with security, safety and compliance for infrastructure and CDN assets being unsupported
- Remediate the technology risks of infrastructure and CDN assets being unsupported

3.1.1.2 Net Present Value (NPV)

The overall 5-year NPV of this option is $1.55M.

3.1.2 Risk Assessment

The specific risks and mitigations associated with not investing in the existing infrastructure and CDN assets are:

Category	Risk	Inherent Risk	Mitigation	Residual Risk
[redacted]	[redacted]	MEDIUM	[redacted]	LOW
[redacted]	[redacted]	HIGH	[redacted]	LOW
[redacted]	[redacted]	MEDIUM	[redacted]	LOW
[redacted]	[redacted]	MEDIUM	[redacted]	LOW

Under the Base Case, the residual risk associated with this approach is illustrated in the table below:

	WHS	Reputation	Compliance	Reliability	Finance	People/IR	Environment	Risk
Likelihood	Likely	Likely	Likely	Likely	Likely	Likely	N/A	LOW
Consequence	Minimal	Minimal	Minimal	Minimal	Minimal	Minimal	N/A	
Risk Level	LOW	LOW	LOW	LOW	LOW	LOW	N/A	

The overall risk rating is LOW with significant positive change in most category risk ratings.

3.2 Option 1 – Replace infrastructure and CDN assets according to vendors' asset life cycle

Option 1 includes the activities described in the Base Case but will refresh CDN assets as recommended by vendors to modernise our CDN and transition it to a next generation network. This option will refresh all infrastructure and CDN assets according to each vendor's asset life cycle.

[redacted]

While this approach will mitigate security and technology vulnerabilities, it does not provide any additional benefits to the business and is more expensive than the Base Case.

3.2.1 Financial summary

The total IT capital expenditure for this option is estimated to be **$24.14M** spread across the five-year regulatory period as shown below:

Table 4: Financial summary – Option 1

IT Capex $m	FY24	FY25	FY26	FY27	FY28	TOTAL
Recurrent costs	$4.17	$6.48	$4.83	$4.87	$3.79	$24.14
Non-recurrent costs	0	0	0	0	0	0
TOTAL	***$4.17***	***$6.48***	***$4.82***	***$4.87***	***$3.78***	***$24.14***

The costs are based on vendor and labour estimates required to deliver the service.

Table 5: Financial summary – Option 1

IT Opex $m	FY24	FY25	FY26	FY27	FY28	TOTAL
Recurrent costs	$0.14	$0.14	$0.14	$0.14	$0.14	$0.70
Non-recurrent costs	0	0	0	0	0	0
TOTAL	***$0.14***	***$0.14***	***$0.14***	***$0.14***	***$0.14***	***$0.70***

In addition, the following benefits have been identified for this option:

3.2.1.1 Quantifiable benefits

Option 1 provides no financial benefits over and above the prudent and efficient continuation of services to the business that, without a reliable CDN, would cause potentially serious disruption to our services to the community.

3.2.1.2 Non-quantifiable benefits

In addition to the Base Case noted above, Option 1 will also:

> Refresh of all infrastructure and CDN assets according to the vendor's asset life cycle.

3.2.1.3 Net Present Value (NPV)

The overall 5-year NPV of this option is -$2.44M.

3.2.2 Risk Assessment

Under the Option 1, the residual risk associated with this approach is illustrated in the table below:

	WHS	Reputation	Compliance	Reliability	Finance	People/IR	Environment	Risk
Likelihood	Likely	Likely	Likely	Likely	Likely	Likely	N/A	LOW
Consequence	Minimal	Minimal	Minimal	Minimal	Minimal	Minimal	N/A	
Risk Level	LOW	LOW	LOW	LOW	LOW	LOW	N/A	

The overall risk rating is LOW with significant positive change in most category risk ratings.

3.3 Options considered and not progressed

Option	Reason for not progressing
Do Nothing	[redacted]

Option	Reason for not progressing
	[redacted]
Maintain only the critical existing infrastructure and CDN assets	[redacted]

4. Evaluation

4.1 Options Evaluation Summary

This OER recommends refreshing the infrastructure and CDN assets to maintain a continuous service into the next regulatory period.

4.2 Commercial Evaluation

The commercial evaluation of the options is set out in the table below.

Table 6: Commercial evaluation

Option	Description	Capex ($m)	Benefits ($m/p.a)	NPV ($m)	Rank
Base Case	Replace infrastructure and CDN assets to maintain a continuous service	$19.28	N/A	$1.55	1
1	Replace infrastructure and CDN assets according to vendor's asset life cycle	$24.14	N/A	-$2.44	2

(Refer to separate costing models for detailed breakdown of these costs)

The above commercial evaluation is based on:

- 4.80% discount
- 5-year asset life

Discount rate sensitivities based on TransGrid's current AER-determined pre-tax real regulatory WACC of 2.23% and 7.37% appear in the table below.

Table 7: Discount rate sensitives

Option	Description	Discount rate at 2.23% NPV $m	Discount rate at 7.37% NPV $m
Base Case	Refresh the infrastructure and CDN assets to maintain a continuous service	$2.20	$0.99
1	Refresh the infrastructure and CDN assets according to vendor's asset life cycle	-$2.22	-$2.62

4.3 Risk assessment

The relative risk assessments of each of the considered options is illustrated in the table below:

Options	WHS	Reputation	Compliance	Reliability	Finance	People/IR	Environment	Risk
Base Case – Refresh infrastructure and CDN assets to maintain a continuous service	LOW	LOW	LOW	LOW	LOW	LOW	N/A	LOW
Option 1 – Refresh infrastructure and CDN assets according to the vendor's asset life cycle	LOW	LOW	LOW	LOW	LOW	LOW	N/A	LOW

5. Preferred Option

This report recommends proceeding with the Base Case – Refresh infrastructure and CDN assets to maintain a continuous service.

The tables below outline the investment, any potential step change in operating costs and the associated benefits of the preferred option.

5.1 Estimated capital costs

Category	Item	Budget ($m)
Material	[redacted]	[redacted]
Labour	[redacted]	[redacted]
Capex Total:		$19.28

5.2 Estimated Opex Step Change

Opex Step Change Year of Change	FY24	FY25	FY26	FY27	FY28	End Of Period
[redacted] (self funded)	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

5.3 Benefits

Benefit	$m/p.a
N/A	
Benefits Total:	$0.00m

*Please note benefit calculations will be refined when each of the projects are scoped in detail.

6. Appendix

[redacted]

[redacted]

[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]		
[redacted]		
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]