Options Evaluation Report (OER)

Employee Enablement

TransGrid

Approvals

Author	Sophong Tran	IT Performance and Governance Associate
Reviewed	Delan Naidu	IT Domain Manager (Technology)
	Marnie Williams	IT Strategy Business Partner
	Andrew Dome	IT Digital Operations and Experience Manager
Approved	Russell Morris	CIO
Date submitted for approval	15 November 2021	

Change history

Revision	Date	Amendment
0.1	April 26 2021	Merged first draft into new updated template with the revised list of initiatives and feedback from Domain lead and Architect
0.2	April 27 2021	Additional updates Sophong Tran
0.3	May 4 2021	Additional updates and feedback from support teams incorporated
0.4	May 4 2021	Migration to new OER template
0.5	May 8 2021	Updates after team walkthrough and review
0.6	May 10 2021	Updated after team review
0.7	May 11 2021	Updated and merged with domain lead comments after team review
0.8	May 12 2021	Clean up comments for draft submission
1.2	August 24 2021	Updated after feedback and revised approach to base option
1.4	Sept 7 2021	Updated for iteration 6 review and incorporate copywriter feedback
1.5	Sept 10 2021	Updated for iteration 6 review and risk tables
1.0	Nov 15 2021	Updated to version 1.0 Nov 15 for the latest submission iteration

Executive summary

This Options Evaluation Report (OER) covers our proposed approach to providing "employee enablement" services, which involves giving our staff the necessary ICT devices (e.g. laptops and iPads), software and telephone services to enable them to do their work and collaborate effectively.

During the current regulatory period, we have seen a tremendous shift in the nature of work in our industry due to restrictions arising from the COVID-19 pandemic requiring remote work. As a result, we have also seen the rise of new collaboration tools, such as Microsoft Teams and Zoom, which are now in mainstream use across the industry.

However, our current software restricts the digital tools available to our employees who, for example, are currently unable to attend Microsoft Teams or Zoom meetings using their work devices. At the same time, a number of core applications that support our enterprise are coming to end of life, when they will be out of vendor support, creating security vulnerabilities, and are becoming increasingly obsolete.

This OER considers two options:

- A Base Case involving a capital refresh that continues our existing approach to procuring and providing employee enablement services to our staff while on premise versions of software remain available.
- Option 1 moving us to a modern workplace by adopting the Office 365 subscription model, rather than having on premise versions of Microsoft Office products. Option 1 also includes migrating to Microsoft Exchange Online and SharePoint Online under the Microsoft 365 licence, in a cost-saving move that will empower our workforce with modern collaboration tools.

We recommend Option 1, which will give our employees access to the most recent software, enabling them to work from anywhere at a lower cost compared with the base case and with a better risk profile. In particular, we estimate the NPV associated with Option 1 is $0.7M better than the base case. This NPV total comes from capex amount for option 1 being $1.4M cheaper but that is partially offset by an increase in opex occurring earlier than the base case.

Table 1: Evaluated options

Component	Base Case	Option 1	Rationale
Devices	Maintain current approach of purchasing and refreshing hardware assets.	Same as Base Case	This will maintain our current prudent approach to refreshing hardware, which we have used consistently across past regulatory periods. Our strategy is to maximise asset value by following vendor refresh cycles, but sweating the assets for a further year or two before refreshing.
Microsoft Office	Refresh to the latest on-premise version of Microsoft Office before eventually moving to Microsoft 365. (This option will delay any opex step change.)	Migrate to Microsoft 365 – an online, subscription-based Software as a Service (SaaS) model	Microsoft's roadmap is moving fully to online version in 2025 and no security updates will be provided for previous versions beyond that. We recommend switching to a subscription approach because it offers better outcomes at similar or better cost levels with a better risk profile. The product will replace current solutions at end of life, while also extending our current capability as part of the refresh. Benefits include increased scalability for a changing workforce, co-

			authoring and collaboration capabilities and Disaster Recovery availability.
Microsoft Exchange email and SharePoint	Maintain existing on-premise solution and moved to the next available version (SharePoint and Exchange 2019) before eventually moving to Office 365.	Move to Microsoft Exchange Online and SharePoint Online under the Microsoft 365 licence.	This offers better reliability and functionality at a lower cost than implementing applications separately as these licences come with the subscription to Microsoft Office 365. It also addresses the security and support issues associated with on-premise Microsoft applications, where support will expire in 2025. By migrating directly to the Microsoft 365 tool suite, all these applications will be supported throughout the next regulatory period.
IP telephony	Move from soon to be decommissioned ISDN solution to SIP solution	Same as Base Case	Our existing ISDN solution is technologically obsolete and will be retired by our telecommunications provider. SIP technology is the industry standard replacement offered by all providers. Apart from a one-time transition cost, the pricing will be net neutral to what we pay today.

Option	Description	Direct Capital cost ($M)	Network & Corporate overheads ($M)	Total Capital cost ($m)	Net Present Value (NPV) ($M)	Rank
Base case	Maintain existing capital refresh approach	[redacted]	[redacted]	$16.038	N/A	2
Option 1	Shift to subscription based services for software	[redacted]	[redacted]	$14.601	$0.7M	1

The proposed capital expenditure for the preferred option, Option 1, is summarised below:

IT Capex $M	FY24	FY25	FY26	FY27	FY28	TOTAL
Recurrent costs	$6.500M	$2.105M	$2.345M	$1.490M	$1.490M	$13.93M
Non-Recurrent costs	$0.643M	$0.029M	$0M	$0M	$0M	$0.671M
TOTAL	$7.143M	$2.134M	$2.345M	$1.490M	$1.490M	$14.601M

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	$4.096M	$1.490M	$2.345M	$1.490M	$1.490M	$10.911M
Non-Recurrent costs	$0.643M	$0.029M	$0M	$0M	$0M	$0.671M
TOTAL	$4.739M	$1.519M	$2.345M	$1.490M	$1.490M	$11.582M

The IFRS impact for this OER is associated with the SaaS solutions associated with the proposed implementation of Microsoft 365 software.

[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 – Why is this important?

Employee enablement services give our staff the necessary ICT devices (e.g. laptops and iPads), software and telephone services to enable them to do their work and collaborate effectively. The modern workplace that we envision for our employees will be a major driver in improving our ability to be responsive, and drive efficiencies and cost savings. But the tools currently available to our employees are becoming increasingly out of date, constraining our workforce's ability to work efficiently and collaboratively.

The COVID-19 pandemic created a rapid and dramatic shift in the way our industry works, with the rise of remote working supported by new collaboration tools. As a result, the last 18 months have highlighted the limitations of our current employment enablement provisioning. For example, our staff are currently unable to attend Microsoft Teams or Zoom meetings using their work devices, preventing them from participating effectively with industry peers and customers.

In addition to no longer being fit for purpose, many of our applications will soon be at end of life, out of support and obsolete.

1.2 Current approach and limitations

1.2.1 Current approach to procuring devices

Our approach to device procurement has been consistently applied through previous regulatory cycles, forming part of our recurrent capex spend. We work with a vendor to manage the provisioning, deployment, maintenance, asset management, return and storage of IT devices such as desktops and laptops. These devices have planned refresh dates within each five-year period on a rolling basis, incurring a large capital investment. We have always been proactive in maximising value from this capital expenditure. Generally, we depreciate assets over three years and then sweat the hardware for an extra one or two years above the recommended hardware manufacturers refresh timeline.

1.2.2 Current Microsoft solutions

Our current versions of Microsoft Office, Exchange (mail server) and SharePoint (enterprise collaboration platform and intranet host) are all located on-premise and will soon lack vendor support:

> Microsoft Office 2016 is at end of life[2]. Although, extended support is currently available, this will expire during the next regulatory period, at which point Microsoft will stop providing patches and security fixes.

> Microsoft Exchange is shifting to a cloud-based model[3] and our current instance of Exchange Mail is residing on ageing hardware infrastructure. We either need to invest in new infrastructure or migrate to a cloud-hosted solution, depending on the best result for our application tool suite and the most prudent use of funding.

[redacted]

[2] https://docs.microsoft.com/en-us/lifecycle/products/microsoft-office-2016

[3] https://www.toolbox.com/collaboration/unified-communications/news/goodbye-on-premise-microsoft-to-shift-office-servers-to-the-cloud/

[4] [redacted]

1.2.3 Current IP Telephony solution

Our telephony solution provider, Telstra, has advised that our current Integrated Services Digital Network (ISDN) will be decommissioned, necessitating a move off this network onto a Session Initiation Protocol (SIP).

Currently, we use fixed voiced services under a previous agreement through the NSW Government Telecommunications Agreement (GTA)[5]. This includes all ISDN lines and PSTN services used at our main office, regional centres and substations. Although GTA ceased in 2015 and is no longer available to any NSW Government department, these rates were maintained for TransGrid pre and post privatisation. In December 2017, as part of our negotiations for mobile services, Telstra agreed as a goodwill gesture to allow TransGrid to remain on ISDN and Option K for fixed voice services on a month-to-month basis to allow transition to a Session Internet Protocol (SIP) solution in due course.

Telstra has been exiting ISDN exit since September 2019, when Category 1 services were disconnected. The final exit date for our Category 3 service will occur over the next one to two years. We therefore need to begin to move off the current ISDN and transition effectively before disconnection occurs during the next regulatory period.

1.3 Consequences of not migrating and refreshing

- **Devices** – To remain functional, ageing hardware eventually needs to be replaced due to wear and tear, technology and performance issues, lost devices and increased incidences of breaking and fixing.
- **Microsoft solutions** – Much like other applications, our Microsoft Office products and collaboration applications have a finite lifecycle. As vendor support expires for obsolete versions, we no longer receive application patches and security updates. As a critical infrastructure provider, we must maintain a level of support to ensure security vulnerabilities are mitigated and core business tools remain supported. Applications therefore need to be periodically refreshed to mitigate technological obsolescence, deteriorating functionality, security vulnerabilities and key personnel skills risk.
- **IP telephony** – We have no alternative available other than to migrate to supported technology. Once Telstra's ISDN services have been decommissioned, we will lose our current IP telephony solution, which is an essential tool for our workforce to communicate both internally and with our partners, peers and customers.

1.4 Risk Drivers

This program aims to address the following risk:

- **Worker Health & Safety:** The integration of our communication and collaboration tools with our business applications help to keep our employees and customers safe and ensure communications to stakeholders are efficient and effective.
- **Reputation:** Our inability to communicate and collaborate effectively with stakeholders and customers has the potential to cause dissatisfaction.
- **Compliance:** Periodic refreshes of our applications are critical to remove and prevent vulnerabilities which allow for unauthorised access to systems and data, leading to business disruption and data loss. A core component of this OER is to mitigate security risks associated with out of support and vulnerable applications.
- **Reliability**: The risk of application failure and vulnerabilities increases exponentially over time and especially as they reach end of life. Extending the life of applications further increases the risk of outages and disruption to business services, including those critical to deliver on essential projects, maintain a reliable network and interact with consumers. Modernising platforms allows better interoperability and reliability.
- **Finance:** When applications age, the cost of maintenance increases. Although, extended support may be purchased, this is costly. It gets to a point where the increased productivity and reduced support costs makes upgrading cheaper than battling on without vendor support. The proposed move to a subscription model is a

[5] Government Telecommunications Agreement (GTA) 2010 "Option K

value-for-money approach that also increases our ability to scale. The move to “Software as a Service” also gives us financial flexibility without a large capital investment.

- **People/IR:** Relying on staff to support ageing applications introduces key-person risk as skills become scare in the market place. Moving to Software as a Service model allows us to make a more efficient use of resources as maintenance activities are built into the cost model.
- **Environment:** N/A

2. Related Needs/Opportunities

Related ICT Programs/OERs. This table describes why this employee enablement OER is important to the other OERs.

ICT Programs/OERs	**Importance to other OERs***	Relationship commentary
Cyber Security	High - Scope	Provides the physical devices that all users utilise.
Data & Decisioning	High - Scope	The implementation of an updated SharePoint solution in this OER will form part of the Data and Decisioning strategy. Provides the devices that these applications use to use these applications
Bespoke Applications	High - Scope	Provides the devices required to use these applications.
Infra. & Network	High - Scope	The Microsoft solutions in this OER will reduce our infrastructure footprint. Provides the devices that connect to our infrastructure and network.
Operational Evolution	High - Scope	Provides the devices required to use these applications.
Customer Safety & Support	High - Scope	Provides the devices required to use these applications.
Application Maintenance	High - Scope	Provides the devices required to use these applications.

* KEY
High – the OER is essential from a functional or compliance perspective to another OER
Medium –the OER is required to fully realise the benefits of another OER or would result in a change in scope
Low – the OER is has a low level of dependency to another OER

3. Options

3.1 Base Case – Maintain existing capital refresh approach

The Base Case will continue our existing approach to procuring and providing employee enablement services to our staff while on-premise versions of software remain available.

3.1.1 Approach to procuring devices

Even with our careful and prudent management of assets, including sweating desktop hardware an extra one to two years on top of the recommended refresh date, the next regulatory submission will require more than a full cycle of device refreshes for end of life hardware. As a result, the Base Case includes significant capital expenditure to replace laptops, desktops and peripheral hardware, such as monitors, keyboards and mouse, docking stations, iPhones and iPads. Projections for this cost are based on an average of the purchases over the past three years.

3.1.2 Approach to refreshing Microsoft Office, Exchange and SharePoint

During the next regulatory period, our current Office and SharePoint tools will reach end of life and no longer receive security updates. To mitigate this risk, the Base Case includes moving to the next available on-premise version of Microsoft Office, likely Office 2019, and refreshing SharePoint and our Exchange Email on-premise solution to the next supported version, likely Microsoft 2019.

This would mitigate vendor support issues and ensure security updates and patches resume until 2025 when Microsoft will cease providing security patches and updates for Microsoft 2019. At this point, we will need to migrate to Microsoft 365.

3.1.3 Approach to procuring our telephony services

With Telstra decommissioning our IDSN services, and no other ISDN solutions available on the market, the only option for providing IP telephony is moving to SIP – the new industry standard. SIP will be an important element of our modern workplace, enabling our employees to use a smartphone, laptop or tablet on the go, or work from home without the need for a landline phone. This solution will help to make us future ready by improving our ability to scale.

3.1.4 Financial summary

The total IT capital expenditure for the Base Case is estimated to be **$16.038M** spread across the five-year regulatory period as shown below:

IT Capex $m	FY24	FY25	FY26	FY27	FY28	TOTAL
Recurrent costs	$6.492	$2.141	$3.725	$1.519	$1.490	$15.367
Non-recurrent costs	$0.671	$0	$0	$0	$0	$0.671
TOTAL	***$7.163***	***$2.141***	***$3.725***	***$1.519***	***$1.490***	***$16.038***

The Base Case will have a delayed opex increase versus Option 1 but will incur increased capital expenditure.

Basis for cost calculations

- **Devices** – based on the actual project costs incurred over the last two regulatory periods in procuring and deploying new devices.
- **Hardware** – based on approximate current market values.
- **Application refresh** – based on previous similar project implementation costs incurred for the last upgrade, with licence costs based on current vendor costs for both on-premise software and monthly subscription services.
- **ISDN to SIP** – based on estimates from our partner and telecommunications vendor.

Please note, the funding for this OER is classified as recurrent costs except for the migration from ISDN to SIP which is a one time cost to move off technology that will be decommissioned by our telco provider.

The basis for our cost calculations apply to both options presented.

3.1.5 Risk Assessment

The specific risks and mitigations associated with the approach to refreshing Microsoft applications in the Base Case are:

Category	Risk	Inherent Risk	Mitigation	Residual Risk
Reliability	Gradual loss of application functionality over time due to performance issues and incompatibility problems with newer products	MEDIUM	Refreshing the platforms in the OER to mitigate the risks associated with outdated technologies and increasing total cost of ownership.	LOW
Compliance	Security updates will no longer be provided by the vendor after current versions reach end of life.	MEDIUM	Refreshing the applications to bring them to the latest supported versions will mean vendors will resume providing security updates and patches for our core business applications. However, extended support will need to be purchased, as Office 2019 will only be supported through 2025 and support beyond that is not guaranteed. The security issue will need to be revisited before 2025 and another refresh may be required.	MEDIUM
Finance	Migrating to the on-premise version of Microsoft tools may not be the best use of capital investment.	MEDIUM	Microsoft has already stated that Office/ SharePoint /Exchange 2019 will be the last products in its roadmap available as vendor-supported, on-premise solutions. From 2025, these products will be continued as a cloud subscription solution through Microsoft 365. At this point, no versions of Microsoft Office, SharePoint or Exchange will receive security patches and support. This option should only be considered if the preference is to delay an opex increase at the cost of a considerably larger capex spend than necessary.	MEDIUM

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	Unlikely	Unlikely	Possibly	Possibly	Possibly	Unlikely	N/A	MEDIUM
Consequence	Minimal	Minimal	Minor	Minimal	Minor	Minimal	N/A	
Risk Level	LOW	LOW	MEDIUM	LOW	MEDIUM	LOW	N/A	

3.2 Option 1 – Shift to subscription based services for software

Option 1 includes the same approaches as the Base Case to device procurement and IP telephony. However, instead of updating our on-premise Microsoft applications where support will expire in 2025[6], we will migrate to the Microsoft 365 tool suite, which will be supported throughout the next regulatory period.

This will allow us to purchase Microsoft Office as a subscription model. It also supports a move to Microsoft Exchange Online and SharePoint Online, as Microsoft 365 comes with these licences. Migrating all three as one initiative, rather than moving them application by application, reduces implementation costs and saves paying for separate licences.

From a functionality point of view, Microsoft 365 will enable employees to access work applications securely from non-TransGrid devices and provide them with collaboration tools, including Microsoft Teams and the ability to co-author documents. It will also ensure business continuity should our corporate network not be available and support better integration between products.

3.2.1 Financial summary

The total IT capital expenditure for this option is estimated to be **$14.601M** spread across the five-year regulatory period as shown below:

IT Capex $m	FY24	FY25	FY26	FY27	FY28	TOTAL
Recurrent costs	$6.500M	$2.105M	$2.345M	$1.490M	$1.490M	$13.93M
Non-Recurrent costs	$0.643M	$0.029M	$0M	$0M	$0M	$0.671M
TOTAL	$0M	$0M	$0M	$0M	$0M	$14.601M

The cost estimates were gathered in the same manner as the Base Case. However, the shift to an opex model as part of this option occurs earlier than the Base Case.

3.2.1.1 Non-quantifiable benefits

Option 1 will:

- Support migration to vendor supported products/versions and remediate the risks associated with using obsolete software and hardware
- Automatically keep Microsoft 365 up to date as part of our subscription service
- Align to our strategy to move to cloud based solutions where appropriate.
- Improve the ability to collaborate across a widely dispersed workforce, from any device anywhere, whilst maintaining the security and integrity of systems and data.
- Support external collaboration by enabling secure document sharing with our customers, suppliers and partners.
- Improve productivity via seamless communication and collaboration across work locations and from home.
- Reduce on-premise infrastructure hosting costs as solutions are migrated to the cloud (built into our solution)

[6] https://www.howtogeek.com/687118/is-your-microsoft-office-still-getting-security-updates/

3.2.1.2 Net Present Value (NPV)

The overall 5-year NPV of this option is $0.7M over the base case.

3.2.2 Risk Assessment

The specific risks and mitigations associated with Option 1 in addition to the Base Case are:

Category	Risk	Inherent Risk	Mitigation	Residual Risk
Reliability	Gradual loss of application functionality over time due to performance issues and incompatibility problems with newer products	MEDIUM	Refreshing the platforms in the OER to mitigate the risks associated with outdated technologies and increasing total cost of ownership.	LOW
Compliance	Security updates will no longer be provided by the vendor after current version reaches end of life.	MEDIUM	Moving to a subscription model will mean the vendor will automatically provide security updates and patches for our core business applications.	LOW

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

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

3.3 Options considered and not progressed

Option	Reason for not progressing
Do Nothing Approach	The Do Nothing approach will not be viable for these initiatives. The reasons are as follows for each > The ongoing hardware device refresh activities have been handled as recurrent capex activities, not opex. It will be impossible for employees to operate as expected if they are working using devices that, during the next regulatory period, would be approaching ten years of age. > Core business applications will be coming to end of life. Though extended support may be purchased, this is costly, the period is finite and does not guarantee security patches to fix vulnerabilities will continue to be provided > The Migration from ISDN to SIP is mandated by Telstra. There are no other same services offered elsewhere as all telco providers are moving

Option	Reason for not progressing
	from this technology. We cannot stay on our current solution without losing our telephony services. This approach is not viable from a risk, service and security perspective so it is not recommended as an option in the proposed OER.
Other Alternatives such as BYOD	As an alternative the desktop hardware refresh options to be looked at, there is a possibility that was considered to allow employees to use a BYOD – "bring your own device" type model whereby the employee would be responsible for acquiring their desktop and laptop hardware. This will enable staff to use whichever devices they prefer without the onus on TransGrid however, there are major unresolved issues with this option including > Security – both physical and device specific security and the requirement to make sure work functions can be performed on these devices while mitigating security concerns > The inability to support different devices types and models and ensure that the same standards and level of functionality apply across the board. > Would there be compensation required to enable staff to purchase devices. Alternative options such as leasing subscription models are available and will need to be looked at further down the line as a possible option. For the purpose of the submission, we recommend that we continue with our existing capital approach with known historical costs.

4. Evaluation

The preferred option, based on the evaluation detailed below is Option 1

4.1 Commercial Evaluation

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

Option	Description	Capex ($M)	Opex ($M)	Benefits ($M/p.a)	NPV ($M)	Rank
Base Case	Maintain existing capital refresh approach	$14.459	[redacted]	$0	N/A	2
Option 1	Shift to subscription based services for software	$13.209	[redacted]	$0	$0.7	1

The above commercial evaluation is based on:

> 4.8% discount

> A five-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.

Option	Description	Discount rate at 2.23% NPV $M	Discount rate at 7.37% NPV $M
Base Case	Maintain existing capital refresh approach	$15.267	$13.725
Option 1	Shift to subscription based services for software	$13.922	$12.563

4.2 Risk assessment

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

	WHS	Reputation	Compliance	Reliability	Finance	People	Environment	Overall Risk Rating
Base Case	LOW	LOW	MEDIUM	LOW	MEDIUM	LOW	N/A	MEDIUM
Option 1	LOW	LOW	LOW	LOW	LOW	LOW	N/A	LOW

4.3 Regulatory Investment Test (RIT-T)

No RIT-T analysis is required under current rules.

5. Preferred Option

This report recommends proceeding with Option 1.

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]
		-
***Direct Capex*:**		[redacted]
Network and Corporate Overheads		[redacted]
Capex Total:		***$14.601***

5.2 Estimated Opex Step Change

Opex Step Change Year over year change	FY24	FY25	FY26	FY27	FY28	End Of Period
Microsoft 365 subscription (self-funded opex)	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

5.3 Benefits

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