Options Evaluation Report (OER)

Application Maintenance

Approvals

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

Change history

Revision	Date	Amendment
0.1	25 April 21	Moved content over to new template from draft version and updated risk information from team.
0.2	6 June 21	Modifications and update with recent template and feedback
0.4	10 Sept 21	Updated formatting and financial view and risk section after feedback
1.0	15 Nov 21	Renamed to version 1.0 for submission and updated IFRS.

Executive summary

Efficiently maintaining and refreshing our applications is critical to avoid compliance and security vulnerabilities, business outages and unnecessary costs. This Options Evaluation Report (OER) covers 93 Commercial off the Shelf (COTS) and Cloud applications that support our business, High Voltage Network and platform. It excludes bespoke applications and applications requiring enhanced capabilities, which are covered throughout the remaining OERs.

As COTS applications typically have a five-year asset life, these applications will reach End of Life (EOL) in the next regulatory period, when they will either be technologically obsolete or no longer supported by our vendors, creating risks across our business.

Our current approach to maintaining COTS applications is to refresh them before they reach EOL. This is based on the recommendations of the ISO16350 framework[1], which suggests taking a risk-based approach for determining an application's life cycle. It is also consistent with industry standards and vendor recommendations.

Our cloud based applications are maintained by the cloud provider as-a-service. This ongoing cost is also included in this submission and forms part of our recurrent opex spend.

Given our existing approach to application maintenance is consistent with industry good practice, we are recommending staying with this base case and have not put forward alternative options. We propose to continue refreshing to the latest supported version, refreshing with a new product (should an application be discontinued) or moving to a cloud based solution where appropriate. Together with investments in the other OERs, this will help us responsibly maintain our security and compliance obligations between 2023-28.

Our proposed allowance for 2023-28 represents a more than 10% reduction when compared to our expected expenditure between 2018-2023. This is because the shift towards cloud based solutions has reduced our overall costs of maintaining and refreshing these applications.

Option	Description	Direct Capital cost ($m)	Network & Corporate overheads ($m)	Total Capital cost ($m)	Net Present Value (NPV) ($m)	Rank
Base Case	**Maintain Current Refresh Approach**	[redacted]	[redacted]	$23.16M	N/A	1

The proposed capital expenditure for this OER is summarised below for the preferred option.

IT Capex $m	FY24	FY25	FY26	FY27	FY28	TOTAL
Recurrent costs	$7.68M	$10.51M	$3.90M	$1.07M	$0M	$23.16M
Non-Recurrent costs	$0M	$0M	$0M	$0M	$0M	$0M
TOTAL	$7.68M	$10.51M	$3.90M	$1.07M	$0M	$23.16M

[1] This ISO16350 framework sets out a framework for the management and maintenance of applications. Further information on this standard is available at https://www.iso.org/standard/57922.html

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[2] 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	$7.68M	$10.51M	$3.90M	$1.07M	$0M	$23.16M
Non-Recurrent costs	$0M	$0M	$0M	$0M	$0M	$0M
TOTAL	$7.68M	$10.51M	$3.90M	$1.07M	$0M	$23.16M

*No expected change for this OER as the forecast is for like for like replacement solutions.

[2] 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. Related Needs/Opportunities

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

ICT Programs/OERs	Importance to other OERs*	Relationship commentary
Cyber Security	Low	The applications refreshed in this OER will need to abide by any security or compliance related requirements introduced in the cybersecurity one.
Data & Decisioning	Low	The use of data by this OER is governed by the data governance framework introduced in the Data OER
Employee Enablement	Low	N/A
Infra. & Network	Medium – Scope	The application maintenance OER and the refresh decisions will impact the infrastructure footprint and network requirements.
Operational Evolution	Low	N/A
Customer Safety & Support	Medium – benefits	Customer Safety and support applications will come under the Application Maintenance OER once transitioned
Bespoke Application Maintenance	N/A	N/A

* 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

2. Context

2.1 Background

2.1.1 Why is this important?

Effective application support, maintenance and renewal is critical to ensure business continuity and service provision to customers, and to secure our technology and data. Unless applications are supported by vendors and up to date throughout their lifecycle, we will be at risk of compliance and security vulnerabilities, technological obsolescence, increased support costs and business disruption (see Section 3.3).

2.2 Overview of current environment and activities

Our business application environment can be categorised into three primary groups: Commercial Of The Shelf (COTS), Bespoke (in-house developed solutions) and Cloud based solutions. The ongoing maintenance activities for all these solutions are covered under our recurrent opex spend.

This OER covers the refresh of our business COTS applications and maintenance of the existing capability on our Cloud applications. It involves no forecasted recurrent capital expenditure. Our Bespoke application refresh is covered under a separate OER submission. The Operational Evolution OER submission covers new capabilities under a non-recurrent capital expenditure request.

Application Category	Number of Applications
COTS [redacted]	***52***
Bespoke [redacted]	***17***
Cloud [redacted]	***41***

Our integration environment is critical to the overall maintenance and support of our applications. This environment is used to ensure applications can work with others in our applications and is critical in testing new applications before they are introduced. Our ICT architecture is moving towards a hybrid solution as we adopt more cloud based applications. Our integration environment will continue to adjust to support both on-premise and virtual models as the move to cloud continues.

Current maintenance approach

We take a prudent approach to maintenance. We refresh our applications before they reach EOL and end of support from vendors, continuing to maintain current application versions and support levels. This ensures applications continue to provide quality services for their full useful life.

Specifically, we align to the ISO16350 standard for application maintenance and refresh, along with vendor recommendations.

> *"ISO 16350:2015 establishes a common framework for application management processes with well-defined terminology that can be referenced by the software industry. It contains processes, activities, and tasks that apply during the stage of operation and use from the point of view of the supplier organisation that enhances, maintains, and renews the application software and the software-related products such as data-structures, architecture, designs, and other documentation. It applies to the supply, maintenance, and renewal of applications, whether performed internally or externally with respect to the organisation that uses the applications."*

This framework has enabled us to maintain good practice in relation to support, patching and security, which we intend to keep through the following five-year regulatory period and refresh cycle.

2.3 Consequences of not maintaining our applications and integration environment

The consequences of not continuing our existing approach to maintaining our applications and integration environment include:

- **Compliance and security vulnerabilities** – To function correctly, applications need vendor support services whenever issues arise that our support teams cannot resolve. Applications under current vendor support also receive regular, ongoing updates and patch fixes as part of day-to-day maintenance. These fixes not only resolve any bugs and functionality-related issues but also incorporate security fixes to rectify vulnerabilities. Given our applications support the high voltage network and transmission business directly and indirectly, they need to be secure, otherwise threat actors can exploit vulnerabilities to access other parts of the network. Vendors are often unwilling to support applications that are not refreshed periodically as outdated applications are built on outdated software. If bugs are no longer being fixed, applications become less available and reliable, compromising compliance.
- **Technological obsolescence** – As applications age, they may no longer be fit for use or warranty to be available to meet business needs. Frequently, older applications are superseded by newer ones that are more robust, meet more stringent security requirements, or conform to newer application architecture standards or changes to application product roadmaps, such as moving to cloud based solutions. As applications are interdependent, in terms of functionality and the transfer of data, a vulnerability in one application can affect them all.
- **Increased support costs** – As technology ages, the support skills available on the market tend to be harder to find and more expensive. By maintaining our applications, we can ensure support skills are accessible and not cost prohibitive. The same concept applies to extended vendor support. Some vendors do offer extended support after a product has reached EOL. However, this usually lasts only a finite period and can be very expensive. This option is only used in a worst case scenario while we upgrade to a supported version.
- **Business disruption** – Our applications support business-critical functions from safety to payroll to finance systems. As applications age and become obsolete, there is an increased risk without refresh that applications will have greater unplanned downtime due to outages & incidents. Recovery times would increase due to applications being unsupported and other possible impacts such as data loss or functionality problems.

2.4 Risk Drivers

The applications under consideration intersect with the following risks:

- **WHS:** Our applications have a direct impact on the safety of the community and staff, in particular those operating in the field. The impact on the community and staff should these applications become unavailable or ineffective due to inadequate maintenance, patching and refresh would be significant.
- **Reputation:** Service and safety failures due to unavailable or ineffective applications have the potential to cause stakeholder dissatisfaction and adverse media coverage for both TransGrid and the broader energy sector.
- **Compliance:** Although vendors maintain applications at a minimal compliance level, this does not equate to Maturity Indicator Level (MIL) security models[3]. Periodically refreshing our applications is critical to preventing unauthorised access to systems and data to support compliance. Refreshing COTS applications that incorporate new features to address compliance obligations is a more efficient option than customising legacy applications ourselves.
- **Reliability**: The risk of application failure and vulnerabilities increases exponentially over time as applications reach EOL as defined the by vendor. Extending the life of applications beyond this point further increases the risk of outages and impacts to business services, including those critical to deliver essential projects, maintain a reliable network and interact with consumers.

[3] https://www.energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf

- **Finance:** When applications age, the cost of maintenance increases as vendors pass on the cost of supporting applications with a shrinking customer base.
- **People/IR:** Persisting with legacy applications entrenches a reliance on obsolete codebases and introduces personnel risks as maintenance skills become scarce.
- **Environment:** N/A

3. Option

3.1 Base case – Maintain Refresh Approach

Given our existing approach is aligned with international standards of good practice, we propose to continue with this approach into the next regulatory period – and have not put forward alternative options in this OER.

The proposed base case is to continue to patch and refresh applications to maintain our security and compliance obligations, with any incremental enhancements made following cost/benefit analysis. Potential actions may involve refreshing to the latest supported version, refreshing with a new product should that application be discontinued or moving to a cloud based solution as the next step of the product roadmap rather than an on premise solution.

This option will refresh all COTS applications as they come to EOL support using a five year average lifecycle – as has been maintained during the past two regulatory periods. The frequency will depend on when new versions, upgrades or applications become available, with priority given to critical applications, noting that the general refresh cycle is every five years for COTS applications. Patching will be completed within a reasonable timeframe to maintain the required levels of security and vendor support.

There is no request for recurrent capex as the current cloud solutions will be maintained under recurrent opex activities to maintain ongoing support to n-1 version releases.

The existing application integration platform will also be maintained and refreshed over the proposed period, similar to the COTS applications.

3.1.1 Financial summary

The total IT capital expenditure for this option is estimated to be **$23.16M** spread across the five-year regulatory period as shown below:

IT Capex $m	FY24	FY25	FY26	FY27	FY28	*TOTAL*
Recurrent costs	$7.679M	$10.507M	$3.901M	$1.073M	$0M	**$23.161M**
Non-Recurrent costs	$0M	$0M	$0M	$0M	$0M	**$0M**
TOTAL	**$7.679M**	**$10.507M**	**$3.901M**	**$1.073M**	**$0M**	**$23.161M**

When developing the cost forecast associated with maintaining and refreshing our COTS applications, the estimates have been based on project work effort actuals from the last refresh of each application. Licence costs are assumed to have be approximately the same as current costs and have carried across to the next regulatory period under the existing opex spend, hence there have been no additional opex requested in this OER as part of the submission.

3.1.2 Net Present Value (NPV)

N/A.

3.1.3 Risk Assessment

We manage the lifecycle of our applications with a view to maximising our investments. This approach has led to strategic decisions to bring forward expenditure on some applications, while extending the life of others where it has been acceptable do so from a risk perspective.

The specific risks and mitigations associated with the base case option are:

Category	Risk	Inherent Risk	Mitigation	Residual Risk
Reliability	Application performance and functionality deteriorates over time without regular maintenance and refresh.	HIGH	Refresh of applications per the application lifecycle of every five years. Refresh of integration environment to correspond to shift in applications to cloud.	LOW
Compliance	Outdated applications will no longer receive security fixes and update, thereby increasing the risk of security vulnerabilities and intrusions.	HIGH	Maintain applications per vendor guidelines to ensure support and patches are made available and the ability to receive 2nd level support from vendors is available if necessary.	LOW
People	Requirement of new skill sets to adapt to new technology and to operate new Generation software	MEDIUM	Refresh to new platforms and codebases to reduce reliance on outdated skillsets. Alleviate key personnel risks associated with support requirements for outdate technologies.	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	Unlikely	Unlikely	Possible	Possible	Unlikely	Possible	N/A	LOW
Consequence	Minor	Minimal	Minor	Minor	Minor	Minimal	N/A	
Risk Level	LOW	LOW	LOW	LOW	LOW	LOW	N/A	

3.2 Options considered and not progressed

Option	Reason for not progressing
Do Nothing Approach	This option will not be functionally capable considering the high level of risks involved. As applications become obsolete, the vendors will stop providing support and critically, security patches and updates. Due to the critical infrastructure operations that TransGrid manages and the underlying ICT application that support these functions, we need to mitigate any risks associated with Security (intrusions, Denial of Services, Malware and vulnerabilities etc.) and deterioration of functionality in our application suite before, during and after the next regulatory period. As applications age, the cost over time increases to support. If we do nothing, the ongoing costs is expected to increase either through more resources required to perform the same level of support or additional costs associated with paying vendors for extended support (the process in which we pay vendors to provide continued support for products that are at end of life). This last option does not guarantee items such as security patches and releases will continue to be provided. Given the discussion above, this is not a viable option and not considered in the OER.
Other Alternatives	The intent of this initiative is to maintain the current services provided by our current IT applications and the refresh of COTS applications as they come to end of life during the next regulatory period. In the planning for COTS refresh options, alternatives may be looked at that time however, application

Option	Reason for not progressing
	roadmaps and solutions are not currently available at the time of this submission. As the regulatory submission process occurs well in advance of when solutions are fully developed, appropriate cost benefit and solutions will be evaluated through the normal project processes to ensure the best solutions are selected when the time comes for each application. There may be options in future that provide greater value for individual applications.

4. Evaluation

4.1 Single Option Evaluation Summary

This OER only presents the existing viable base case to maintain our current applications into the next regulatory period.

4.2 Commercial Evaluation

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

Option	Capex ($M)	Benefits ($m/p.a)	NPV ($m)	PVR	Rank
Base Case – Maintain Current Refresh Approach	$20.545	N/A	N/A	N/A	1

The above commercial evaluation is based on:

> 4.8% discount

> An asset life of 5 years for COTS applications

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 Refresh Approach** - Support and maintain current applications including those being established as part of Digital Core program - Refresh COTS applications and one dependent bespoke application based on 5-year EOL average. - Minor enhancements only for Bespoke applications - Continue migration of integration platform	$21.88M	$19.35M

5. Preferred Option

This report recommends proceeding with Base Case.

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]
		[redacted]
***Direct Capex*:**		[redacted]
Network and Corporate Overheads		[redacted]
Capex Total:		*$23.16M*

5.2 Estimated Opex Step Change

Opex Step Change Year over year change	FY24	FY25	FY26	FY27	FY28	End Of Period
Additional FTE support (self funded)	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

5.3 Benefits

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