Options Evaluation Report (OER)

Bespoke Application Refresh

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	05 November 2021	

Change history

Revision	Date	Amendment
0.1	16 June 2021	Initial
1.0	05 Nov 2021	Completed submission to Reg team

Executive summary

This Options Evaluation Report (OER) assesses the options for ensuring our outdated and obsolete Bespoke applications are appropriately developed, maintained and modernised. It covers 17 legacy Bespoke applications performing functions critical to meeting our cybersecurity obligations and complying with National Electricity Rules on meter management, billing, outage planning and communication.

Changes to technology and the regulatory landscape mean these applications are no longer fit for use. As some applications will be up to 15 years old by the start of the next regulatory period, they are also becoming increasingly expensive and challenging to maintain. ███████████████████████████████████████ ██ ████████████████████████████████████

This OER considers two options to refresh and maintain our Bespoke applications:

1. The Base Case will upgrade and modify the existing legacy code base to align it to the current supported version. This will involve performing extensive testing to make sure it will still integrate with current applications and platforms. We will also remediate security vulnerabilities and retrofit the various changes. This option will involve extensive testing and re-testing, and require additional headcount to remediate and maintain security compliance. Eventually, the base case will require another complete refresh as obsolete technology fails to provide adequate functionality or meet our compliance requirements.

2. Option 1 will refresh our bespoke applications using a modern code base that will not quickly become obsolete (unlike the code in the Base Case). The applications will be refreshed using security by design, allowing greater ability to respond to current and future requirements. This option will allow us to remove the cost requirement to bring on an additional security resource to manage application support.

Both options propose implementing a modern Devops[1] development platform, with up-to-date security controls, testing and tooling, to ensure our COTS[2] and Bespoke application development adheres to best practice industry standards and guidelines.

Component	Base case	Option 1	Justification for Option 1
Development environment	Implement a secure environment	Same as the Base Case	Required to mitigate the current and evolving cyber coding vulnerabilities
Refresh of bespoke apps	In place upgrade of software retaining code base	Refresh software with modern code base	Bespoke applications will reach their end of life in the next period. A move to a modern code base will ensure applications do not run on unsupported code base

Our preferred option, Option 1, will not only fully remediate the problem of outdated technology but will also decrease the future cost of support, improve security compliance and support a lower risk profile.

---

[1] https://en.wikipedia.org/wiki/DevOps

[2] Commercial Off The Shelf applications covered in the *Application Maintenance OER*

TransGrid

Table 1: Evaluated options

Option	Description	Direct Capital cost ($M)	Network & Corporate overheads ($M)	Total Capital cost ($M)	Net Present Value (NPV) ($M)	Rank
Base case	In place upgrade of all bespoke applications and implement Development environment	███████	█████	$17.694	N/A	2
Option 1	Recode and refresh all Bespoke applications and implement Development environment	█████	██████	$21.589	$9.769	1

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

IT Capex $M	FY24	FY25	FY26	FY27	FY28	TOTAL
Recurrent costs	$4.498M	$5.052M	$4.696M	$2.036M	$0M	$16.282M
Non-Recurrent costs	$0.526M	$0.263M	$2.026M	$1.351M	$1.140M	$5.307M
TOTAL	$5.024M	$5.315M	$6.723M	$3.385M	$1.140	$21.589M

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[3] 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	$4.498M	$5.052M	$4.696M	$2.036M	$0M	$16.282M
Non-Recurrent costs	$0.526M	$0.263M	$2.026M	$1.351M	$1.140M	$5.307M
TOTAL	$5.024M	$5.315M	$6.723M	$3.385M	$1.140	$21.589M

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

---

[3] 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.

TransGrid

1. Context

1.1 Background

1.1.1.1 Current situation with Bespoke applications

We have 17 legacy Bespoke applications that are becoming obsolete and will reach of end of life in the next regulatory period.

Over 15 years, we have developed these applications to overcome the shortcomings of COTS applications. Bespoke applications perform critical functions enabling key business activities, such as: planning and tracking outages to High Voltage equipment; supporting protection relays; maintaining metering equipment and customer billing; and identifying safety risks.

Similar to COTS applications, we maintain our Bespoke applications by performing patching and upgrades to keep them current and up-to-date with security patches and fixes. This basic maintenance work is covered in the *Application Maintenance OER* through ongoing opex spend to replace like-for-like functionality.

██
██
████████████████████████████████████. The cost of maintaining ageing applications is also rising as maintenance skills become scarce. This forces us to find obsolete skills at increasingly expensive prices and also introduces key person risk.

Importantly, it is becoming increasingly hard to upgrade Bespoke applications to remain compliant with cybersecurity regulations and meet functionality and availability requirements. ██████████████████
██
████████████████████████████████████

1.1.1.2 Current situation with development environment

Our current development platforms for Bespoke and COTS applications are inadequate and require modernisation.
██
██
██
████████████████████████████████████

In the changing dynamics of our industry, we are also increasingly working with third party vendors to provide more efficient and scalable solutions to benefit our consumers. This requires having a device agnostic platform and APIs for integration. Otherwise, we will be faced with costly workarounds to provide external services using applications designed for internal consumption.

Modern security and application coding standards offer us a much more economical way to refresh our applications, using a "security by design" method to incorporate requirements into a new application – rather than continually trying to retrofit the existing code to meet our obligations. This approach is consistent with a recent maturity assessment on our testing environment, which recommended implementing the modern development platform similar to that proposed by this OER.

1.1.2 Why is this important?

Funding was not sought to upgrade these applications in the current regulatory period as our prudent management has extended the life of these applications to 7 to 10 years – longer than equivalent COTS applications. However,

---

[4] ██
████████████████████████████████████

TransGrid

refreshes are now essential to avoid the risk and cost associated with having critical applications running on unsupported and outdated technology.

The option proposed in this OER will:

> Refresh, re-platform and modernise bespoke applications to bring them back to supportable levels. This will support the performance and continuity of functions critical to meeting our cybersecurity obligations and complying with National Electricity Rules on meter management, billing, outage planning and communication.

> Set up secure coding tools, a development platform and frameworks for all of bespoke and COTS applications to allow current and future development. This will move us to a more scalable, automated and on-demand development model, allowing us to respond to changing security requirements and technology, and evolutions in the energy market and government regulations.

1.2   Risk Drivers

This program aims to address the following risks:

> **WHS:** Our Bespoke applications have a direct impact on the welfare and 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:** We use Bespoke applications to comply with the National Electricity Rules (NER) ███████ ██ ██ ██.

> **Reliability**: The risk of application failure and vulnerabilities increases exponentially over time and as they reach end-of-life. Extending the life of applications further increases the risk of outages and impacts to business services, including those critical to deliver on essential projects, maintain a reliable electricity network and interact with consumers. Modernising platforms allows for better interoperability and reliability with newer technologies.

> **Finance:** When applications age, the cost of maintenance increases. This is particularly true of Bespoke applications, which generally have a longer lifecycle, where the scarce skills required to support these technologies become increasingly more expensive.

> **People/IR:** Persisting with legacy applications entrenches a reliance on obsolete codebases and introduces personnel risks as skills availability diminishes. The current staffing model is under resourced, putting at risk the 24/7 availability model of our critical bespoke applications.

> **Environment:** N/A.

███/

TransGrid

2.   Related Needs/Opportunities

Related ICT Programs/OERs. This table describes why this bespoke 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 solutions proposed in the bespoke OERs and where they are hosted, will have a direct impact to the footprint of our infrastructure, whether they will be in our data centres or in public or private clouds.
Operational Evolution	Low	N/A.
Customer Safety & Support	Medium – benefits	Includes one bespoke application (TSS) not covered in this OER.
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

TransGrid

3.   Options

3.1   Base case – In place upgrade of all bespoke applications and implement Development environment

The Base Case involves upgrading and refreshing 17[6] Bespoke applications within the existing legacy code base ▮▮▮▮▮▮▮▮▮▮

This will require significant work, even if we continue to use the existing code base. Integrating Bespoke applications into the new development environment and tooling will be challenging, especially to address security vulnerabilities and upgrade the coding components, technologies and frameworks.

The risk of effecting existing functionality during this process is high. Each layer of changes will need to be applied one-by-one. Teams will need to stop to test each change layer, re-test functionality and adjust if it is not working as expected. This process of testing and retesting is expected to be more extensive than building the code from scratch in a modern environment with inbuilt technology components and frameworks.

The upgrade and refresh of Bespoke applications will also require existing interfaces with other applications to be updated and reconfigured.

Both the Base Case and Option 1 will put in place a modern development environment with security controls, testing and tooling as part of a Devops[7] development platform. This will ensure our COTS and Bespoke application development adheres to updated best practice industry standards and guidelines. The new development environment will provide us with:

> A Continuous Integration/Continuous Deployment (CI/CD) pipeline.

> Secure offshore development environments

> Automation in both code promotion and testing

> DevSecOps to integrate and build in security testing within the CD pipeline.

> Secure offshore development environments

> Data Governance Operations to manage customised data (secure/filtering/masking)

> A scalable development environment to meet the changing needs of the industry and customers while only paying for what is used rather than investing in development infrastructure

> A reduced capital footprint for our development environment

> A reduction to the overall security risk for applications, as they will be developed in an environment with inbuilt security tooling and principles from the beginning, ensuring the design and code is compliant as it is developed and addressing issues earlier before the cost of redesigns grows

3.1.1   Financial summary

The total IT capital expenditure for this option is estimated to be $17.649M spread across the five-year regulatory period as shown below:

▮▮▮.

[7] https://en.wikipedia.org/wiki/DevOps

TransGrid

IT Capex $m	FY24	FY25	FY26	FY27	FY28	*TOTAL*
Recurrent costs	$1.208M	$3.150M	$4.161M	$2.643M	$1.506M	*$12.668M*
Non-Recurrent costs	$1.034M	$0M	$1.710M	$1.141M	$1.141M	*$5.026M*
TOTAL	*$2.242M*	*$3.150M*	*$5.871M*	*$3.784M*	*$2.647M*	*$17.694M*

As Bespoke applications have a 7 to 10 year lifecycle, investing only in critical enhancements during the current regulatory period ▓▓▓▓▓▓▓▓ Hence they are due for remediation over the next regulatory cycle.

Costs for both options are based on a bottoms-up estimate using previous iterations of upgrades and function point analysis[8] as well as sourced vendor quotes.

3.1.1.1 Quantifiable benefits

N/A

3.1.1.2 Non-quantifiable benefits

N/A

3.1.1.3 Net Present Value (NPV)

N/A.

3.1.2 Risk Assessment

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

Category	Risk	Inherent Risk	Mitigation	Residual Risk
Reliability	Today, testing each application involves multiple development environments and manual work.	MEDIUM	A modern DevOps type platform will enable a secure, consistent, automated approach, supporting a better quality product and greater efficiency throughout the development lifecycle. The refreshed applications will run on supported software, enabling vendor support and easier integration with other modern applications.	LOW
Reliability	Not refreshing the platforms and applications included in the OER, will fail to address the risks associated with outdated technologies, resulting in our failure to comply with relevant standards, obligations and audit outcomes.	MEDIUM	Refreshing the platforms in the OER will mitigate the risks associated with outdated technologies.	LOW

---

[8] https://www.tutorialspoint.com/estimation_techniques/estimation_techniques_fp_counting_process.htm

TransGrid

Category	Risk	Inherent Risk	Mitigation	Residual Risk
People/IR	Not refreshing to new platforms and codebases increases reliance on outdated skillsets.	MEDIUM	Refreshing to new platforms and codebases reduces reliance on outdated skillsets. However, the ongoing management and support of the modern technologies, components and new security standards will require an increase in resources to support and manage.	MEDIUM
Finance	Total Cost of Ownership for Bespoke applications increases as older technology becomes more difficult to support and harder to integrate with newer technology. This may culminate in us being unable to comply with its regulatory and commercial requirements, leading to fines.	MEDIUM	Refreshing and modernising the Bespoke applications to supportable levels should mitigate the frequency and length of application outages. However, significant costs are associated with remediating the applications using the current code base. Each change will need to be tested thoroughly before the next layer of changes is applied. This amount of testing is much higher than required to redevelop the applications on an upgraded development tool using new security tools. Upgrading to newer technologies will extend the ability to fulfil our future compliance obligations. However, reengineering the current code base, rather than rebuilding it, runs the risk that some applications may still reach a point where they can no longer be remediated and a full or partial redevelopment may be required.	MEDIUM
WHS	Bespoke applications are core to our worker safety and management of our transmission facilities.	MEDIUM	Modernising Bespoke platforms should mitigate the risk of outages due to obsolete technology and running critical applications on an unsupported platform.	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	Unlikely	Possible	Possible	N/A	MEDIUM
Consequence	Moderate	Minimal	Minor	Minor	Moderate	Minor	N/A	
Risk Level	LOW	LOW	LOW	LOW	MEDIUM	MEDIUM	N/A	

3.2 Option 1 – Recode and refresh all Bespoke applications and implement Development environment

Option 1 will also implement the modern development environment outlined in the Base Case. However, this option differs by upgrading and refreshing the 17 bespoke applications ███████████████ using a modern code base, rather than the outdated code proposed in the Base Case. This approach would:

> Remove the requirement to have skilled resources to support obsolete technology available and the associated costs of these skills on the market

> Remove the Base Case risk associated with sinking investment into code that cannot be used for the expected remaining life of the applications

TransGrid

> Reduce the testing and verification effort needed, over that in the base case, to implement the same security and supportability compliance.

3.2.1   Financial summary

The total IT capital expenditure for the Option 1 is estimated to be $21.589M spread across the five-year regulatory period as shown below:

IT Capex $m	FY24	FY25	FY26	FY27	FY28	TOTAL
Recurrent costs	$4.498M	$5.052M	$4.696M	$2.036M	$0M	$16.282M
Non-Recurrent costs	$0.526M	$0.263M	$2.026M	$1.351M	$1.140M	$5.307M
TOTAL	$5.024M	$5.315M	$6.723M	$3.385M	$1.140	$21.589M

These costs are based on a bottoms-up estimate using previous iterations of upgrades and function point analysis[9] as well as sourced vendor quotes.

3.2.1.1   Quantifiable benefits

N/A

3.2.1.2   Non-quantifiable benefits

In comparison to the base case, Option 1 will:

> Remediate and refresh of all bespoke applications to bring them to supported software versions

> Reduce key personnel and skills risk required to support obsolete software

3.2.1.3   Net Present Value (NPV)

The overall 5 year NPV of this option is $9.769M 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	Today, testing each application involves multiple development environments and manual work.	MEDIUM	A modern DevOps type platform will enable a secure, consistent, automated approach, supporting a better quality product and create efficiency throughout the development lifecycle. The refreshed applications will be running on supported software, enabling vendor support and easier integration with other modern applications.	LOW
People/IR	Refresh to new platforms and codebases reduces reliance on outdated skillsets.	LOW	Modernise and re-align our skills to efficiently support our bespoke applications. Remove key person risks of needed the skills to support obsolete resources in the team.	LOW

---

[9] https://www.tutorialspoint.com/estimation_techniques/estimation_techniques_fp_counting_process.htm

TransGrid

Finance	Ongoing maintenance costs of the current development environments are costly and labour intensive.	MEDIUM	Modernising the Development platforms will set up future savings in terms of capital investment and the ongoing support of development environments. The infrastructure footprint can be reduced by moving to a cloud utility model.	LOW
WHS	Bespoke applications are core to our worker safety and management of our transmission facilities.	MEDIUM	Modernising Bespoke platforms should mitigate the risk of outages due to obsolete technology and running critical applications on an unsupported platform.	LOW

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	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	N/A	LOW
Consequence	Minimal	Minimal	Minor	Minor	Minor	Minor	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	Technically, we are able to do nothing with our bespoke applications and continue the ongoing maintenance without performing a refresh. However, it introduces a high level of risks in terms of security, safety and regulatory issues. These applications perform most of our critical functions ███████ ███ ██ and regulatory compliance functions that are not available from commercial applications. These applications have been maintained for the past two regulatory periods without any modernisation activities and now require to be brought to current technologies to mitigate the technology and security risks.

Currently, we don't have a development environment that is capable of meeting our current or future needs. ███████████████████████████ █████████████████████████████████. In its current state, we will not be able to handle the requirements that we know are coming to support the forecasted TransGrid network activities and the expansion into renewable energy.

Given the above, we consider that the do nothing option is not functionally capable and should not be considered in further detail on the OER. |
| **Others** | This initiative covers the recurrent capex spend. Due to not performing any refresh activities on our bespoke applications during the previous two regulatory periods, we do not consider there are other alternative options that would provide the required functionality and mitigate risks associated with aging technology and from a security vulnerability perspective. |

TransGrid

Option	Reason for not progressing
	There may be however, when these initiatives are further scoped for refresh activities that alternative solutions are available that may make a better investment during the next regulatory period, such as possible cheaper commercial alternatives become available, consolidation of applications or functions etc. As these are unknown at this time from a commercial, functional or technological perspective, it is recommended that these are evaluated again for each application during the detailed scoping design phase.

Other options considered include refreshing only certain critical bespoke applications however, this still left security vulnerabilities that would need to be addressed in the remainder of the applications and the level of risks associated with this approach have been considered too high to move forward with. |

TransGrid

4. Evaluation

4.1 Options Evaluation Summary

4.1.1 Preferred Option

The preferred option is Option 1 which will create a modern development environment and:

> Remediate security, safety and compliance risks associated with critical bespoke applications being unsupported.

> Remediate the technology risk of critical bespoke applications being unsupported.

> Remediate the personnel risks associated with skills required to support outdated software.

> Have a better NPV than the base option

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)	Rank
In place upgrade of all bespoke applications and implement Development environment	$15.339	N/A	N/A	2
Recode and refresh all Bespoke applications and implement Development environment	$19.184	N/A	$9.769	1

The above commercial evaluation is based on a 4.8% discount.

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	In place upgrade of all bespoke applications and implement Development environment	$16.538	$14.266
Option 1	Recode and refresh all Bespoke applications and implement Development environment	$20.415	$18.069

4.3 Risk assessment

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

TransGrid

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

TransGrid

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	██████████████████	███
Labour	████████████	███
		█
Direct Capex:		███
Network and Corporate Overheads		███
Capex Total:		***$21.589***

5.2 Estimated Opex Step Change

Opex Step Change	FY24	FY25	FY26	FY27	FY28	End Of Period
Development Environment run costs (self-funded)		████████████████████████████████████				

5.3 Benefits

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

TransGrid

████████████	███████████████████████	██████
████████████████████ ████████████	██████████████████████████████████ ████	
█████████████████████████ ██████████████ █████████████	██████████████████████ ██████████████	████████████████
██████ ████████████████████	█████████████████████████████████████	████████████████████
██████████████████ ████	███████████████████████████████	████████████████ ██████████
██████████████ █████████████████████ ████████████		

██
██
████████████████

██
█████████████████████████████████

███████████	█████████████	██████████████████████████████████
█████████████ ████████	████████████████ █████████████████████ ██████████	███████████████████████████████████████ ███ ██████████████████████████████████████ █████████████████ ████████████████████████████████████ ████████████████████████████████████ ███████████████████ ████████████████████████████ ██████████████████████████████████ ███████████████████████████ █████████████████████████████ ████████████████████████████████ ████████████████████████████

▬▬▬ ▬▬▬▬	▬▬▬▬▬▬▬ ▬▬▬	▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬
▬▬▬	▬▬▬▬▬▬▬▬▬ ▬▬	▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬
▬▬▬▬	▬▬▬▬▬▬▬▬▬▬	▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬
▬▬▬▬▬	▬▬▬▬▬▬▬▬▬▬▬	▬▬▬▬
▬▬	▬▬▬▬▬▬▬▬▬▬	▬▬▬▬▬
	▬▬▬	▬▬▬▬▬▬▬▬▬
		▬▬▬▬
		▬▬▬▬▬▬▬▬▬
		▬▬▬▬▬▬▬▬▬
		▬▬▬▬▬▬▬▬▬▬
		▬▬▬▬▬▬▬▬▬▬▬
		▬▬▬▬▬
		▬▬▬▬▬▬▬▬
▬▬▬ ▬▬▬	▬▬▬▬▬▬▬ ▬	▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬
▬▬▬	▬▬▬▬▬▬▬▬▬▬▬	▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬
▬▬▬	▬▬▬▬▬▬▬▬▬▬	▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬
	▬▬▬▬▬▬▬▬▬▬▬	▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬
	▬▬▬▬▬▬▬▬▬▬▬	▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬
	▬▬▬▬▬▬▬▬▬	▬▬▬▬
	▬▬▬▬▬▬▬	▬▬▬▬▬▬▬▬▬▬
	▬▬▬▬▬▬▬▬▬	▬▬▬▬
	▬▬▬▬▬▬	▬▬▬▬▬▬▬▬▬▬
	▬▬▬▬▬▬▬▬	▬▬▬▬▬▬▬
		▬▬▬▬▬▬▬▬▬
		▬▬▬▬▬▬▬▬▬▬
		▬▬▬▬▬
		▬▬▬▬▬▬▬▬
▬▬▬▬▬▬▬	▬▬▬▬▬▬▬ ▬	▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬
	▬▬▬▬▬▬▬▬	▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬
	▬▬	▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬
		▬▬▬▬▬▬▬▬▬
		▬▬▬▬
		▬▬▬▬▬▬▬▬
		▬▬▬▬▬▬▬▬
		▬▬▬▬▬▬▬▬▬
		▬▬▬▬▬▬▬▬▬
		▬▬▬▬▬

TransGrid

████████	████████	████████████████████████
		████████████████████
████████ ████████ ████████ ████	████████ ████████ ████████ ████████ ████	████████████████████ ████████████████████ ████████████████████ ████████ ████████████████ ████████████ ████████████████████ ████████████████████ ███████ ████████████████
████ ████████ ████	████ ████████████ ████████ ████████ ████ ████████ ████████████ ████████	████████████████████ ████████████ ████████ ████████████████ ████████████ ████████████████████ ████████████████████████ ████ ████████████████
████████ ████ ████████ ████ ████	████████ ████████ ████████ ████ ████████████ ████████ ████	████████████████████████ ████████████████████████ ████████████████████████ ████████████████████████ ████████████████████ ████████████████████████
████████████ ████ ████ ████ ██	████████████████ ████████ ████████ ████	████████████████████████ ████████████████████████ ████████████████████ ████████████ ████████ ████████████ ████████████ ████████████████ ████████████████████ ████

TransGrid

██████████	██████████████	████████████████████████████
██████████ ███████████ ████	████████████████ ██████████ ██████████ ████████████ ██████████ ████████████ ███████	██ ████████████████████████████ ████████████████████████
████████████ ████████████	████████████████ ████████████████ ████████████████ ██████████ ████████████ ██████████ ██████████ ████████████ ██████████ ██████████ ██████████	████████████████████████████ ████████████████████████ ██████████████████████████ ████████████████████████ ████████
████████ ██████ ████████ ████ ████	████████████ ████████████ ████████████ ████████████ ████	████████████████████████ ██████████████████████████ ██████████████████████████ ██████████████████████████ ██████████████████████████ ████████████████████████ ████████████████████████

TransGrid