E2E - Stage 2 options analysis (project initiation)

TN-IES-SAP ENHANCEMENTS PROGRAM - DEC 22 (IES)

❖*For work being proposed for inclusion into the capital works program.*

Project name:	ERP Upgrades and Enhancements
Department:	Technology & Performance
Investment Type:	Non-Network
Investment Category:	Non-Network - Information Technology
Functional Area(s):	ITSSC
Project ZoNe location:	assetzone.tnad.tasnetworks.com.au/R24_distribution/ICTIT
Document Number:	R0002079179
Needs Item Reference:	R0002119290
Regulatory Investment Test Required?	No
Version Number:	1.0
Date:	15/12/2022

❖

Preferred Option:			Option 1		
Level 1 Estimate +/- 30 per cent (preferred option – base dollars):			$13,379,115		
Expenditure profile	FY25	FY26	FY27	FY28	FY29
Capex	$ 2,675,823	$ 2,675,823	$ 2,675,823	$ 2,675,823	$ 2,675,823
Opex					

❖

Sign-offs (in support of the recommended option)			
Works Initiator:	David Sales	Date	30/10/2021
Leader: (Endorsement)	Hayley Sheppard	Date	23/02/2022
Leader or General manager noting delegation levels. (Approval)[1]	Andrew Davis	Date	Click here and type the date.

[1] Approval based on delegation level.

❖ denotes mandatory field

1. RELATED DOCUMENTS

Description	URL
Needs Form	R24_NEE_S_IT_ITSSC_SAP Enhancements Program - Needs Assessment
Estimate	R24_EST_S_IT_ITSSC_SAP_Upgrades_and_Enhancements_-_Project_Cost_Model_-_Option_1_-_V2.xlsm R24_EST_S_IT_ITSSC_SAP_Upgrades_and_Enhancements_-_Project_Cost_Model_-_Option_2_-_V2.xlsm
NPV	R24_NPV_S_IT_ITSSC_SAP_UG_and_Enhancement_Pgm_-_NPV_-_V3.xlsx
Asset Management Plan	IT Software Asset Management Plan
TasNetworks Towards 2030	
TasNetworks Digital Strategy	
Future Distribution System Vision	
TasNetworks Corporate Plan	
TasNetworks Business Plan	
TasNetworks Risk Management Framework	
National Electricity Rules (NER)	

2. OVERVIEW

2.1 BACKGROUND

TasNetworks utilises SAP as its digital core, powering business processes including enterprise resource planning functionality spanning payroll, human resources, supply chain, finance, enterprise asset management and project management. The solution has introduced numerous benefits in the form of standardised business processes, provision of accurate and real-time information and facilitated the decommissioning of numerous legacy applications.

As TasNetworks continues to strive for operational improvements and business transformation through new technologies, there is a need for the upgrade of the SAP Core ERP system to the latest release S/4HANA and to upgrade a range of associated modules to the latest versions.

2.2 PROBLEM DEFINITION

There is a need to perform a variety of upgrades to the ERP suite over the course of the Reset period on order to maintain standard support for the product. This is critical to resolve any failures in the systems and to maintain compliance with changes in legislation, agreements or policy. For example Payroll regulations such as single-touch payroll, and reflecting changes from Enterprise agreements amongst others.

Minor enhancements are also required to improve usability and increase efficiency, for example Enhancing the NAO (Network access order) process, optimising the creation of asset master data, refining materials and assemblies to improve the job estimation process.

The following table shows the end of support dates for key components of the ERP suite.

Blue stars show the end of Mainstream Maintenance where Extended Maintenance or Customer Specific Maintenance is available.

Red stars show the end dates for Extended Maintenance or for Mainstream Maintenance where Extended Maintenance is not available.

After the Red stars the only support available is the limited Customer Specific Support package. This effectively restricts support to dealing with situations where the system stops working. Such events may incur additional charges.

Customer specific Support does not provide updates for legal or regulatory compliance. Amongst other constraints, it also provides no guarantee of compatibility with updated database or operating system versions, excludes support for any new interfaces, and provides no service level agreement. Consequently it exposes TasNetworks to significant risk of failure or non-compliance.

[redacted]

3. CUSTOMER NEEDS AND IMPACT

TasNetworks staff need access to supported, compliant and functional software that is appropriate for their role. Not maintaining systems as recommended will impact on our ability to deliver efficient and effective services to external customers. It also introduces the risk of failure of critical systems and increases support costs.

A wide range of consultation has taken place, including meetings and email conversations, to assess the needs of system owners and impacts on system users.

4. CORPORATE ALIGNMENT❖

4.1 BUSINESS PERFORMANCE OBJECTIVES

This project will help achieve the customer and business performance objectives in TasNetworks' Corporate Plan, and as shown in Table 1.

Table 1 - Performance objectives relevant to this project.

Performance Category	Performance Measure	Investment impact on performance
Our business - Sustained cost management	Efficient capital expenditure.	The proposed initiative will apply the most cost-effective option available to maintain the ERP suite supported and consistent with regulatory requirements.
Our business - Network service	Works program delivered	The ERP suite is integral to delivery of the works program. Maintaining it in a supported and healthy state will enabling that.
Our customers	Customer satisfaction	The ERP suite is integral to delivery of the works program in a satisfactory way to meet customer needs. Maintaining it in a supported state will enabling that, though it may miss some opportunities for efficiency and enhanced functionality.
Safety and wellbeing	Reportable incidents	The proper functioning of certain ERP components (such as Plant Maintenance and HCM) is important for maintaining personal safety for staff.
Our people	Employee engagement	Maintaining properly operational systems without the need for manual workarounds is important to maintain staff moral and

Performance Category	Performance Measure	Investment impact on performance
		wellbeing. Failure or inadequate functioning of these systems could quickly put employees under significant additional workload stress.
Our business - Sustained cost management	Operational expenditure	Upgrading systems to ensure regulatory compliance avoids operational costs resulting from manual workarounds and other inefficiencies in system usage.

4.2 RISK OBJECTIVES

The corporate plan identifies a number of business risks outlined in the TasNetworks Risk Framework. The TasNetworks Risk Appetite Statement details the level of risk the business finds acceptable in each category (Safety, Environmental, Financial, Regulatory, Legal and Compliance, Customers, Assets, Reputation and People).

This initiative addresses Regulatory Compliance, Safety and Customer risks, of which TasNetworks has **No** to **Limited** appetite. Not updating systems in line with recommendations introduces the possibility of systems failing, leaving employees within the business unable to fulfil their roles, including effectively providing external and internal customer service. Not updating TasNetworks systems will also impact on the underlying infrastructure, which will be unable to be upgraded leaving it open to failure and security vulnerabilities.

An assessment of the risks mitigated by the project is presented in Section 6.3 and further detail in Appendix B – Key Business Risk Comparison.

Table 2 - Business risks mitigated by this project

Risk ID	Risk category	Risk	Impact
ITR-187	Regulatory, Legal and Compliance	Not improving systems as recommended will mean we cannot adjust to changes in policy and regulation, for example in payroll / superannuation regulations and enterprise agreements.	TasNetworks may damage relationships with regulators or be subject to sanctions for non-compliance with regulation or enterprise agreements.
ITR-188	Customer-Focus	Not maintaining the ERP suite as recommended will impact on our ability to deliver efficient and effective services to external customers.	Loss of productivity and engagement from not utilising an up-to-date ERP suite.
ITR-189	Customer Focus	Not maintaining systems introduces the risk of failure of critical systems such as the ERP suite.	Failure of business critical systems will result in the business being unable to fulfil their roles and be able to provide services to both internal and external customers.
ITR-190	Business Continuity Management	If not maintained in a healthy supported state, the current systems may suffer degraded performance, data loss or complete failure, which would impact on the continuity of various critical business functions.	Negative impacts on TasNetworks' operations, or failure of ability to operate in some areas.
ITR-191	Death or Injury (Employee)	The proper functioning of some ERP components (such as Plant Maintenance and HCM) is important for maintaining personal safety for staff.	Systems could fail or malfunction which would result in an increased risk of staff personal injury or death.

Risk ID	Risk category	Risk	Impact
ITR-192	Cyber Security	If applications and associated operating systems are not maintained in a healthy supported state, they become more vulnerable to Cyber Attacks. The need for manual interventions to overcome functional gaps also increases the risk of Cyber Attacks.	Compromised systems could result in significant financial loss. It could also cause significant disruption or total failure of our ability to process market transactions with resultant impact on customers and reputation.
ITR-193	Cyber Security	If systems are not maintained in a healthy supported state, they become more vulnerable to Cyber Attacks. A compromised business system could also act as an entry point to the whole of TasNetworks IT Ecosystem.	A cyber attack that affects multiple operational systems could cause widespread disruption to the business, breeches of market obligations and release of sensitive data.

4.3 STRATEGIC OBJECTIVES

The following table summarises strategic objectives that will be addressed by this project.

Table 3 - Strategic objectives relevant to this project

Strategic Document	Strategic Objective	How the proposed investment will address the strategic goal
TasNetworks Business Plan	**Our Business** – "Deliver our Works Programs"	Should health of the ERP suite decay, its ability to support effective delivery of our Works Program will diminish. This initiative aims to keep systems supported and healthy.
TasNetworks Business Plan	**Our Owners** – "Driving an efficient business that ensures our business remains sustainable"	Healthy TasNetworks business applications and IT infrastructure are essential to ensure efficient operation of the business. If they are not adequately maintained their ability to support the business will diminish.
TasNetworks Business Plan	**Our Customers** – "We engage with our customers, and continue to develop customer-centric approaches"	TasNetworks ERP suite supports the business's ability to perform a variety of customer facing functions. Not maintaining support could lead to adverse customer impacts. This initiative aims to keep systems supported and healthy.
TasNetworks Business Plan	We will fail to "Enable our workforce for a changing future" by retaining outdated tools that don't meet the needs of the business today or into the future.	Enabling our workforce requires the availability of contemporary supported IT systems. If we fail to take advantage of advances in technology and/or allow critical systems to become unsupported we are not properly enabling the workforce.
Digital Technology Strategy	"Get the most out of ERP" "Treat Data as an Asset" "Digitise processes to be operationally efficient" "Accelerate and Increase the impact of digital"	• In order to get the most out of ERP, it must be maintained in a healthy supported state. • Up-to-date systems allow us to properly manage our data and maximise its utilisation. • Up-to-date contemporary ERP tools will facilitate operational efficiency • Up-to-date contemporary ERP tools will avoid the need to revert to paper based processes.

5. PROJECT OBJECTIVES❖

The objective of the project is to upgrade various ERP modules over the 2024-29 period so that at the end of the period all modules are still under standard support arrangements and TasNetworks is not paying for extended support/maintenance arrangements.

A key component of this process is to [redacted] A number other modules will be upgraded either before or after this major change, based on dependencies as follows.

- [redacted]
  - [redacted]
  - [redacted]
- [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
- [redacted]

6. OPTIONS ANALYSIS❖

6.1 OPTIONS CONSIDERED AND ECONOMIC ANALYSIS

Table 4 lists the options considered, the outcome of the economic analysis for each option, and the option being proposed for endorsement in this Investment Evaluation Summary. Details of the NPV analysis are included in Appendix A.

Table 4 - Options considered

Option No.	Option summary	Direct 5yr cost ($m)	NPV ($m)	Preferred option (yes/no)	Reason for selection/rejection
0	Do nothing, i.e. No ERP upgrades or enhancements	$30.11	$(53.38)	No	This is not recommended as it will lead to degradation of critical systems and business capability as well as legal and regulatory non-compliance.
1	Minimal ERP Upgrades and Compliance Enhancements	$13.38	$(23.72)	Yes	Maintains system support and regulatory compliance at minimal cost
2	UPGRADE ALL OF THE ERP COMPONENTS IN A TIMELY MANNER	$18.26m	$(32.34)	No	Significantly more costly with small additional benefit.

6.1.1 OPTION 0: DO NOTHING – NO ERP UPGRADES OR ENHANCEMENTS

The option of 'Do Nothing' assesses the scenario where this initiative is not approved. It assumes that if funding is not allocated to apply any SAP system upgrades.

If system versions are not maintained, TasNetworks systems will become non-compliant, out of date and lose support, leading to increased cost and compliance risks. Systems will become progressively non-compliant with policy and regulation changes for example in payroll / superannuation regulations and modifications to reflect enterprise agreements.

TasNetworks will need manual workarounds for various processes, such as payroll processing. These workarounds will have significant costs and negative impact to the business.

Customer specific support packages may be available for some ERP modules but these will typically cover only system breakdown and not adaption to new regulations.

Table 5: Option 0 – Scenario Assessment

Criteria	Advantages	Disadvantages
Solution effectiveness		If this initiative does not progress, critical business systems will not be maintained in a healthy, supported state.
Cost	No initial CAPEX cost to consider.	TasNetworks will need to pay a premium for extended support of the systems where this is available. Others may partially or fully fail, requiring manual workarounds or replacement with alternate products.
Business impact		Failure or temporary unavailability or these critical systems would cause severe impact to various areas of TasNetworks including Works Management, Asset Management, Finance and Payroll.
Business strategic alignment		This has low strategic alignment. The business objectives identified in section 4.3 would not be supported.
IT strategic alignment		This option conflicts with the IT principle that systems shall be maintained in a healthy and supported state. If the 'Do Nothing' option is selected, the systems may become inefficient and fail, and thus cease to be fit for purpose.
Project complexity	N/A	N/A
Risk		See Appendix B – Key Business Risk Comparison
Compliance		TasNetworks' critical business systems would become progressively non-compliant with policy and regulation changes for example in payroll / superannuation regulations and enterprise agreements. They would also not be compliant with the vendor's support requirements.
Time	N/A	N/A

6.1.2 Option 1: Minimal ERP Upgrades and Compliance Enhancements

This option entails performing the minimum upgrades of ERP modules as necessary to maintain compliance with policy and regulation changes for example in payroll / superannuation regulations and enterprise agreements. This involves applying support packs where available and implementing regulatory enhancements where these are not provided in the support packs.

Table 6: Option 1 – Scenario Assessment

Criteria	Advantages	Disadvantages
Solution effectiveness	Critical systems will remain supported.	
Cost	This option has the lowest capital cost consistent with maintaining regulatory systems compliance. This option delays the capital cost of migration to [redacted] until the next reset period.	This option incurs additional Customer Specific Maintenance costs to support
Business impact	The business will maintain regulatory compliance.	The business will not get access to new application features when they are made available and will miss opportunities to improve the business efficiency and effectiveness.
Business strategic alignment	It will provide partial support for the strategy and performance objectives detailed in sections 4.1 and 4.3.	
IT strategic alignment	This option will align with the IT strategy components that say applications: • Will be maintainable and supported. • Will align with current IT infrastructure. • Will align with other IT roadmap initiatives.	This option will not align with the IT strategy components that says applications: • Are designed to suit TasNetworks work practices and work processes so as to be as efficient and effective as possible without compromise. Without taking advantage of all available enhancements, some opportunities for efficient and effective operations may be forfeited.
Project complexity	This option is assessed as having lower complexity than option 2 because it involves minor upgrades.	However, it is simply delaying the complexity of an inevitable significant upgrade.
Risk Profile	This option provides a reasonable degree of risk mitigation. See Appendix B – Key Business Risk Comparison.	
Compliance	This option will ensure the ERP suite is compliant with any changing policy and regulation.	
Time	This option would span the full reset period, dealing with Service Packs and Regulatory Changes as they arise.	

6.1.3 Option 2: Upgrade all of the ERP components in a timely manner

This option entails upgrading all of the ERP components in a timely manner during the reset period such that by the end of 2029 all are up-to-date and covered by Mainstream (Standard) Maintenance.

This brings forward upgrade costs that will need to be incurred eventually, but it would also provide a range of useability and functionality advantages over option 1.

The biggest component of the upgrade would be the migration of the Core ERP components to the new [redacted] platform. This includes the following modules

[redacted]

Human Resources and Payroll (HCM) is also part of the Core ERP, but is the subject of a separate proposal to migrate into the SuccessFactors Employee Central product. If that proposal is not approved, then the HCM module will need to be included in the migration to [redacted]

Various other modules of the ERP suite need to be migrated to newer versions or replacement products, including:

[redacted]

[redacted] to occur prior to execution, both in regard to the core migration and also the other products. The migration / upgrade strategy for dealing with non-core products may affect the approach and timing of the core migration.

Some of the non-core products are already out of mainstream maintenance cover and do not have the option of extended support. It would be desirable to upgrade these as soon as possible, but it may be more cost effective to upgrade them at the same time as, or after the [redacted]

The key benefits offered by this option are based on reducing the risk of significant disruption to the organisation by the failure of critical systems that are not supported by the vendor.

Table 7: Option 2 – Scenario Assessment

Criteria	Advantages	Disadvantages
Solution effectiveness	Critical systems will remain supported.	
Cost	This option has a lower long term cost as all of the upgrades that it includes will be required eventually and it avoids some of the Extended Maintenance cost associated with option 0 and option 2. (Assuming neutral licence changeover for [redacted].)	Compared with options 0 and 1, the inevitable capital cost is incurred earlier.
Business impact	The business will get access to new application features when they are made available and will gain opportunities to improve the business efficiency and effectiveness.	
Business strategic alignment	It will support the strategy and performance objectives detailed in Sections 4.1. and 4.3.	
IT strategic alignment	This option will align with the IT strategy, specifically that applications: • Are designed to suit TasNetworks work practices and work processes so as to be as efficient and effective as possible without compromise. • Will be maintainable and supported. • Will align with current IT infrastructure. • Will align with other IT roadmap initiatives.	
Project complexity		The project for this option will be more complex than option 1.
Risk Profile	This option has the greatest risk minimisation impact. See Appendix B – Key Business Risk Comparison.	
Compliance	This option will ensure the ERP suite is compliant with any changing policy and regulation. It would also maintain compliance with the vendor's support requirements.	
Time	This option provides more time for a structured and orderly approach to the multiple upgrade activities required and avoids a rushed upgrade to [redacted] when it becomes essential.	

6.1.4 Sensitivity Analysis

N/A

6.2 OPTION EXPENDITURE PROFILES

The following tables show the expenditure profile for each investment option.

Option 0 – Do nothing Estimate (in nominal dollars) $30.11m					
Expenditure profile	FY25	FY26	FY27	FY28	FY29
Capex					
Opex	$6,022,343	$6,022,343	$6,022,343	$6,022,343	$6,022,343

Option 1 – Minimal ERP Upgrade For Regulatory Compliance Estimate (in nominal dollars) $13.38m					
Expenditure profile	FY25	FY26	FY27	FY28	FY29
Capex	$2,675,823	$2,675,823	$2,675,823	$2,675,823	$2,675,823
Opex					

Option 2 – Upgrade all of the ERP components in a timely manner Estimate (in nominal dollars) $18.26m					
Expenditure profile	FY25	FY26	FY27	FY28	FY29
Capex	$3,649,130	$3,649,130	$3,649,130	$3,649,130	$3,649,130
Opex					

6.3 RISK MITIGATION

Remaining on older software technologies can impact the range of platforms and interfaces that are compatible and can impact on infrastructure upgrades. The matrix below provides a comparison of each option's impact against the company risks identified in section 3.3 "Risk objectives"). Appendix B contains supporting details of the risk assessment outcomes as summarised in Table 8 - Risk Matrix summary.

Table 8 - Risk Matrix summary

Risk ID	Risk Category	Risk Drivers	Impact	Option 0 Gross risk	Option 1 Net risk	Option 2 Net risk
ITR-187	Regulatory, Legal and Compliance	Not improving systems as recommended will mean we cannot adjust to changes in policy and regulation, for example in payroll /	TasNetworks may damage relationships with regulators or be subject to sanctions for non-compliance with	High	Medium	Medium

Risk ID	Risk Category	Risk Drivers	Impact	Option 0 Gross risk	Option 1 Net risk	Option 2 Net risk
		superannuation regulations and enterprise agreements.	regulation or enterprise agreements.	🟥	🟨	🟨
ITR-188	Customer-Focus	Not maintaining the ERP suite as recommended will impact on our ability to deliver efficient and effective services to external customers.	Loss of employee productivity and engagement will impact on customer service.	Medium	Medium	Low
ITR-189	Customer Focus	Not maintaining systems introduces the risk of failure of critical systems such as the ERP suite.	Failure of business critical systems will result in the business being unable to fulfil their roles and be able to provide services to both internal and external customers.	Medium	Low	Low
ITR-190	Business Continuity Management	If not maintained in a healthy supported state, the current systems may suffer degraded performance, data loss or complete failure, which would impact on the continuity of various critical business functions.	Negative impacts on TasNetworks' operations, or failure of ability to operate in some areas.	High	Medium	Medium
ITR-191	Death or Injury (Employee)	The proper functioning of some ERP components (such as Plant Maintenance and HCM) is important for maintaining personal safety for staff.	Systems could fail or malfunction which would result in an increased risk of staff personal injury or death.	Medium	Medium	Medium
ITR-192	Cyber Security	If applications and associated operating systems are not maintained in a healthy supported state, they become more vulnerable to Cyber Attacks. The need for manual interventions to overcome functional gaps also increases the risk of Cyber Attacks.	Compromised systems could result in significant financial loss. It could also cause significant disruption or total failure of our ability to process market transactions with resultant impact on customers and reputation.	[redacted]	[redacted]	[redacted]
ITR-193	Cyber Security	If systems are not maintained in a healthy supported state, they become more vulnerable to Cyber Attacks. A compromised business system could also act as an entry point to the whole of TasNetworks IT Ecosystem.	A cyber attack that affects multiple operational systems could cause widespread disruption to the business, breeches of market obligations and release of sensitive data.	[redacted]	[redacted]	[redacted]

6.4 QUANTITATIVE RISK ANALYSIS

N/A

6.5 BENCHMARKING

N/A

6.6 EXPERT FINDINGS

N/A

6.7 PREFERRED OPTION

The preferred option is to perform the minimum upgrades of ERP modules as necessary to maintain compliance with policy and regulation changes for example in payroll / superannuation regulations and enterprise agreements. This involves applying support packs where available and implementing regulatory enhancements where these are not provided in the support packs.

This option does not include the migration of the Core ERP components to the new S/4HANA platform. Rather, it assumes that TasNetworks takes advantage of the Extended Maintenance that SAP has announced will be available on the core ERP modules for the period 2017 to 2030. That extended maintenance includes the availability of regulatory and legal compliance updates.

Some of the non-core products are already out of mainstream maintenance cover and do not have the option of extended support. If regulatory changes arise that impact any of these components, they would need to be upgraded to supported versions. If regulatory changes don't impact them, there will still be a risk of failure.

This initiative supports a range of business strategies and objectives as identified in Sections 4.1 and 4.3 above.

7. INVESTMENT TIMING❖

Detailed sequencing of upgrades will be the subject of a planning process yet to be completed.

However the timing is expected to be approximately as shown below.

Indicative SAP Upgrade Timeline

[redacted]

8. EXPECTED OUTCOMES AND BENEFITS

The desired outcome of this initiative is an up-to-date ERP suite that fully supports the business and is properly supported by the vendor.

The key benefits offered are based on reducing the risk of significant disruption to the organisation by the failure of critical systems that are not supported by the vendor. More detail is provided in Table 8 above and in Appendix B – Key Business Risk Comparison.

A timely upgrade process will also limit the need to pay Extended Maintenance or costly Customer Specific Maintenance charges to extend vendor support after Mainstream Maintenance ends.

Business benefits will also be derived from improved efficiency and functionality offered in the upgraded ERP modules. Unfortunately insufficient information is available at present on which of the new functionality will be implemented in order to quantify the benefit.

9. ASSUMPTIONS ❖

The table below shows the assumptions used for this IES.

Table 8 - Assumptions

ID	Assumption Description
ITA-001	Cost estimates used on the analysis have a level of accuracy of ±30% and do not include the 20% contingency amount applicable to this type of project.
ITA-151	It is assumed that the separate proposal to migrate HCM into the SuccessFactors Employee Central product is approved, which means the HCM module does not need to be included in the [redacted]
ITA-152	It is assumed that the ERP vendor product policy, licensing and maintenance dates do not change significantly prior to commencing this initiative.

ID	Assumption Description
ITA-161	If no compliance upgrades are performed, Payroll will require manual workarounds to ensure compliance.
ITA-162	There will be additional Premium Support Costs.
ITA-163	If HCM changes are not applied for organisational changes, various processes including approvals will break.
ITA-164	Without SSL certificates maintained cloud components will cease to function.
ITA-165	Without adjusting cost structures to suit changes in financial modelling, time will be wasted on manually compiling and reporting financial data.
ITA-166	Without minor performance enhancements, time is wasted on workaround processes, due to back-end and front-end issues.

10. REGULATORY INVESTMENT TEST

N/A

11. RECOMMENDATION ❖

It is recommended that the preferred option is approved and progressed as it best satisfies the customer and business needs.

12. APPENDIX A – ECONOMIC ANALYSIS

The assumptions used in the economic analysis are as follows:

- NPV analysis is carried out for a 10 year period from the start of the initiative.
- Weighted Average cost of Capital (WACC) of 2.79 per cent is used.

The results of the Economic Analysis are provided below:

ANALYSIS OF OPTIONS		Option 0	Option 1	Option 2
		Status Quo - Do Nothing	Minimal upgrades & compliance enhancements	Upgrades and Usability Enhancements
CASHFLOW	*flow*			
Capital Expenditure	Cash outflow	-	(26,758,230)	(36,491,300)
Operational Expenditure	Cash outflow	(60,223,435)	-	-
Operational Cost savings	Cash Inflow	-	-	-
Total Expenditure	Cash outflow	(60,223,435)	(26,758,230)	(36,491,300)
Revenue	Cash Inflow	-	-	-
Net Cashflow	Net cash	(60,223,435)	(26,758,230)	(36,491,300)
CASHFLOW NPV		(53,379,796)	(23,717,493)	(32,344,521)
PLUS NON CASH				
Non Cash Benefits	Non cash in	-	-	-
Non Cash Costs	Non cash out	-	-	-
Net Value	Net Value	(60,223,435)	(26,758,230)	(36,491,300)
COST BENEFIT NPV		(53,379,796)	(23,717,493)	(32,344,521)
	RANKING	3	1	2

13. APPENDIX B – KEY BUSINESS RISK COMPARISON

The project options each have a different impact on key business risks. The table below provides a qualitative summary of the impacts of each option on key business risks, with consideration for the risk approach and risk management process outlined in TasNetworks' Risk Management Framework.

Risk ID	Risk Category	Impact	Option 0 – Do Nothing				Option 1 – Minimal ERP Upgrade For Regulatory Compliance				Option 2 – Upgrade all of the ERP components in a timely manner			
			Likelihood	Consequence	Risk	Mitigation	Likelihood	Consequence	Risk	Mitigation	Likelihood	Consequence	Risk	Mitigation
ITR-187	Regulatory, Legal and Compliance	Not improving systems as recommended will mean we cannot adjust to changes in policy and regulation, for example in payroll / superannuation regulations and enterprise agreements. This may damage relationships with regulators or result in sanctions for non-compliance.	Likely	Major	High	Unmitigated	Unlikely	Major	Medium	Maintaining critical systems in a healthy state and under standard vendor maintenance will reduce the risk of disruption or failure.	Unlikely	Major	Medium	Maintaining critical systems in a healthy state and under standard vendor maintenance will reduce the risk of disruption or failure.
ITR-188	Customer-Focus	Not maintaining the ERP suite as recommended will impact on our ability to deliver efficient and effective services to external customers.	Possible	Moderate	Medium	Unmitigated	Rare	Moderate	Medium	Maintaining critical systems under standard vendor maintenance will reduce the risk of disruption or failure but not take advantage of some opportunities for additional functionality and efficiency improvements.	Rare	Moderate	Low	Maintaining critical systems in a healthy state and under standard vendor maintenance will reduce the risk of disruption or failure.
ITR-189	Customer Focus	Not maintaining systems introduces the risk of failure of critical systems such as the ERP suite.	Possible	Moderate	Medium	Unmitigated	Rare	Moderate	Low	Maintaining critical systems in a healthy state and under standard vendor maintenance will reduce the risk of disruption or failure.	Rare	Moderate	Low	Maintaining critical systems in a healthy state and under standard vendor maintenance will reduce the risk of disruption or failure.
ITR-190	Business Continuity Management	If not maintained in a healthy supported state, the current systems may suffer degraded performance, data loss or complete failure, which would impact on the continuity of various critical business functions.	Possible	Major	High	Unmitigated	Unlikely	Major	Medium	Maintaining critical systems in a healthy state and under standard vendor maintenance will reduce the risk of disruption or failure.	Unlikely	Major	Medium	Maintaining critical systems in a healthy state and under standard vendor maintenance will reduce the risk of disruption or failure.
ITR-191	Death or Injury (Employee)	The proper functioning of some ERP components (such as Plant Maintenance and HCM) is important for maintaining personal safety for staff.	Unlikely	Major	Medium	Unmitigated	Rare	Major	Medium	Maintaining critical systems in a healthy state and under standard vendor maintenance will reduce the risk of disruption or failure.	Rare	Major	Medium	Maintaining critical systems in a healthy state and under standard vendor maintenance will reduce the risk of disruption or failure.
ITR-192	Cyber Security	If applications and associated operating systems are not maintained in a healthy supported state, they become more vulnerable to Cyber Attack. The need for manual interventions to overcome functional gaps also increases the risk of Cyber Attack.	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Maintaining critical systems in a healthy state and under standard vendor maintenance will reduce the risk of disruption or failure.	[redacted]	[redacted]	[redacted]	Maintaining critical systems in a healthy state and under standard vendor maintenance will reduce the risk of disruption or failure.

Risk ID	Risk Category	Impact	Option 0 – Do Nothing				**Option 1 – Minimal ERP Upgrade For Regulatory Compliance**				Option 2 – Upgrade all of the ERP components in a timely manner			
			Likelihood	Consequence	Risk	Mitigation	Likelihood	Consequence	Risk	Mitigation	Likelihood	Consequence	Risk	Mitigation
ITR-193	Cyber Security	If systems are not maintained in a healthy supported state, they become more vulnerable to Cyber Attack. A compromised business system could also act as an entry point to the whole of TasNetworks IT Ecosystem causing widespread disruption to the business, breeches of market obligations and release of sensitive data.	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Maintaining critical systems in a healthy state and under standard vendor maintenance will reduce the risk of disruption or failure.	[redacted]	[redacted]	[redacted]	Maintaining critical systems in a healthy state and under standard vendor maintenance will reduce the risk of disruption or failure.