Investment Evaluation Summary (IES) IT.INF.08

Project Details:

Project Name:	[redacted]
Project Id:	IT.INF.08
Thread:	IT Infrastructure
CAPEX / OPEX:	CAPEX + OPEX
Scope Type:	C
Service Classification:	Alternate Control
Work Category Code:	AMITS
Work Category Description:	IT Software General – Standard Control
Project File Location:	DD17 Infrastructure
Preferred Option Description:	[redacted]

	17/18	18/19	19/20	20/21	21/22	22/23	23/24	24/25	25/26	26/27
Estimate ($M)	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		[redacted]	[redacted]
Total ($) 2017-2019	[redacted]									
Total ($) 2017-2027	[redacted]									

Governance:

Project Initiator:	[redacted]		
Thread Approved:	[redacted]		
Project Approver:	[redacted]	**Date:**	< APPROVALTIMESTAMP>

Document Details:

Version Number:	1.0

Section 1 (Gated Investment Step 1)

1. Background

This Investment Evaluation Summary (IES) documents planned expenditures for the determination period for [redacted]. The document is one of eight planned documents covering anticipated activities as described in the IT Infrastructure Asset Management Plan.

Effective and timely provision of [redacted] is essential to the continued availability and integrity of TasNetworks IT service delivery. These services are provided at TasNetworks through a variety of platforms and processes, including both hardware and software components. The services can be broken into a number of broad sections (with some overlap):

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

For more information regarding the platforms in use at TasNetworks, refer to the IT Infrastructure Asset Management Plan.

It is expected and assumed that current versions of hardware and software infrastructure underpinning delivery of these services will remain largely as-is in the lead up to the determination period:

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

The initiative scope is documented in detail below in Scope, at a high level the document scope extends to:

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

1.1 Investment Need

Investment drivers fall into the following categories:

1. Reliable and effective delivery of IT services to the TasNetworks business and external customers.
2. Compliance with state and federal legislative and regulatory requirements, including:
    a. Industry-specific requirements
    b. State and federal privacy legislation
    c. Occupational Health and Safety requirements
3. The need to maximise the efficiency and cost-effectiveness of service delivery.

Activities and requirements driving the need for capital expenditure in this IES are documented in Section 4 of the IT Infrastructure Asset Management Plan. To summarise, [redacted] upgrade and replacement activities will arise from:

1. Lifecycle replacement and capacity management activities.
2. Requirements to maintain appropriate levels of software assurance and vendor technical support.
3. Implementation of new functions and capabilities.

1.2 Customer Needs or Impact

TasNetworks IT infrastructure is critical to the reliable, timely and effective delivery of business application and data services to operational and administrative staff. These services are directly related to TasNetworks ability to deliver efficient and effective services to our external customers [redacted]

The Corporate IT department is strongly focussed on service delivery to internal customers. These services are delivered in a manner that aligns with TasNetworks mission, commitments and values. The customer consultation program for the Infrastructure Program of Work documented in this IES reflects an approach of constant and direct engagement with business customers through:

- Regular direct meetings with management teams from all business units at least every six months. These meetings are broadly scoped and cover all services provided by Corporate IT as well as discussing current and emerging requirements from the business.
- A formal project prioritisation process that includes full transparency, extensive customer consultation and business-determined priorities.
- A fully consultative project management methodology that embeds Corporate IT customers in every stage of the project.

1.3 Regulatory Considerations

The effective management, monitoring and maintenance of [redacted] is critical to ensuring that TasNetworks meets its regulatory obligations under:

- Federal Privacy Act (1988)
- Tasmanian Personal Information and Protection Act (2004)
- Tasmanian Anti-Discrimination Act (1998)

Finally, the platforms documented in this Initiative Statement host applications and data used by TasNetworks staff in day-to-day operational and administrative processes. These processes are critical to ensuring business compliance with regulatory requirements.

2. Project Objectives

The primary objective of this initiative is to ensure TasNetworks ability to deliver prescribed, negotiated and non-prescribed services to customers. This objective is achieved through meeting the following initiative objectives:

1. Provide [redacted] as documented to ensure the availability and integrity of TasNetworks applications and data through the determination period
2. Take advantage of technology advances to improve the scope and performance of service delivery to the business
3. Ensure that all software in use is licensed appropriately
4. Ensure that business application services are operated to meet TasNetworks compliance requirements for data privacy and data retention.
5. Ensure the integrity and confidentiality of TasNetworks data
6. Protect TasNetworks IT infrastructure against targeted attacks
7. Block unwanted, offensive and malicious content from entering the network [redacted]
9. Detect and respond to security incidents in order to correct damage and evaluate incidents that have occurred.

The objectives will be met through the execution of maintenance, review, upgrade and replacement activities as described below.

3. Strategic Alignment

3.1 Business Objectives

The following table highlights the problems that the initiative will solve.

Strategic Goal	Problems this initiative will address
"we enable our people to deliver value"	• The activities proposed in this initiative help to ensure a stable platform to support all IT systems.

"we care for our assets, delivering safe and reliable network services while transforming our business"	• There is substantial risk of doing nothing (see chapter titled 'Current Risk Evaluation'). • 'Do nothing' means TasNetworks IT may fail its remit to provide effective and efficient business systems solutions.

3.2 Business Initiatives

The activity proposed in this initiative underpins most other IT activity as it supports the security of almost all IT systems.

4. Current Risk Evaluation

The TasNetworks Risk Framework details the level of risk the business finds acceptable in each category (Safety & People, Financial, Customer, Regulatory Compliance, Network Performance, Reputation and Environment & Community).

This initiative addresses Regulatory Compliance and Reputational risks, of which TasNetworks has a **No** to **Limited** appetite.

Failure to maintain appropriate [redacted]

4.1 5x5 Risk Matrix

TasNetworks business risks are analysed utilising the 5x5 corporate risk matrix, as outlined in TasNetworks Risk Management Framework.

Relevant strategic business risk factors that apply are follows:

Risk Category	Risk	Impact	Likelihood	Consequence
Regulatory Compliance	[redacted]	[redacted]	Possible	Moderate
Reputation	[redacted]	[redacted]	Possible	Major

Section 1 Approvals (Gated Investment Step 1)

Project Initiator:	[Enter name]	Date	
Line Manager:	[Enter name]	Date	

Manager (Network projects) or Group/Business Manager (Non-network projects):	[Enter name]	Date	
[Send this signed and endorsed Summary to the Capital Works Program Coordinator.]			

Actions			
CWP Project Manager commenced initiation:	[Enter date here]	Assigned CW Project Manager:	[Enter name here]
PI notified project initiation commenced:	[Enter date here]	Actioned by:	[Enter name here]

Section 2 (Gated Investment Step 2)

5. Preferred Option

The preferred option is for TasNetworks IT to continue management and maintenance of IT security platforms to ensure the availability, integrity and confidentiality of TasNetworks application and data services.

Risks associated with not proceeding with this option include:

- Increased risk of service disruption [redacted] of TasNetworks IT systems
- Increased risk of regulatory breaches due to [redacted]

Potential business impacts associated with these risks include:

- [redacted]
- [redacted]
- Delays to business operations arising from interruptions to or degraded performance of business applications
- Penalties arising from breaches of regulatory responsibilities

The program of work documented below represents the preferred option for continued delivery of IT security services in support of business activities and initiatives.

5.1 Scope

The scope of this initiative encompasses the following items:

Item	Description/Notes
[redacted]	[redacted]

Project Activity	Schedule	Description
[redacted]	[redacted]	[redacted]

[redacted]

5.2 Expected outcomes and benefits

Activities and requirements driving the need for capital expenditure in this IES are documented in Section 5 of the IT Infrastructure Asset Management Plan. To summarise, activities will fall into the following categories:

- Operational support and maintenance of security hardware and software platforms
- Upgrade and refresh of security hardware and software platforms
- Ensure the integrity and confidentiality of TasNetworks data
- Protect TasNetworks IT infrastructure against targeted attacks
- Block unwanted, offensive and malicious content from entering the corporate network;
- Provide secure and reliable remote access over un-trusted public networks; and
- Detect and respond to security incidents in order to correct damage and evaluate incidents that have occurred.
- Effectively respond to security incidents

Implementation of the recommended option will ensure that security systems maintained and replaced in accordance with the Asset Management Plan, and that the associated software is appropriately licensed and supported.

5.3 Regulatory Test

N/A

6. Options Analysis

This option matrix provides a comparison of the options against the investment drivers detailed in section 2.

6.1 Option Summary

Option 0 – Do Nothing

Continue to use existing systems until failure

Criteria	Advantages	Disadvantages
Solution effectiveness		Unable to keep pace with evolving threat landscape
Cost	Reduced CAPEX	Increased OPEX
Business impact		Increased risk of service outages due to security breaches
Business strategic alignment		
IT strategic alignment		Does not align with IT strategy
Project complexity	N/A	
Risk profile		Increased risk of security breaches
Ability to achieve compliance		Potentially unable to maintain adequate security controls due to technological obsolescence
Time - ability to implement within a deadline	N/A	

Option 1 – Recommended Option

Upgrade and replace security systems as documented

Criteria	Advantages	Disadvantages
Solution effectiveness	Able to keep pace with changing threat landscape	
Cost		Moderate cost
Business impact	Lower likelihood of service outages due to security breaches	
Business strategic alignment		
IT strategic alignment	Aligns with IT strategy	
Project complexity		Low to moderate project complexity spread throughout the determination period
Risk profile	Reduces risk of service disruption	
Ability to achieve compliance	Better able to maintain adequate security controls	
Time - ability to implement within a deadline		May require vendor/integrator assistance to implement some projects

Option 2 – Defer [redacted]

Operate [redacted] over a longer lifespan, deferring upgrade activity accordingly

Criteria	Advantages	Disadvantages
Solution effectiveness	More able to keep pace with changing threat landscape than Do Nothing	Less able to keep pace than Preferred
Cost		Lower cost than Preferred
Business impact		Higher likelihood of service outages due to security breaches (compared to Preferred)
Business strategic alignment		
IT strategic alignment	Aligns with IT strategy	
Project complexity		Low to moderate project complexity spread throughout the determination period
Risk profile		Slightly higher risk of disruption than Preferred
Ability to achieve compliance	Better able to maintain adequate security controls than Do Nothing	
Time - ability to implement within a deadline		May require vendor/integrator assistance to implement some projects

6.2 Summary of Drivers

Criteria	Option 0	Option 1	Option 2
Solution effectiveness			
Cost			
Business Impact			
Business strategic alignment	N/A	N/A	N/A
IT strategic alignment			
Project complexity	N/A		
Risk profile			
Ability to achieve compliance			
Time - ability to implement within a deadline	N/A		

6.3 Summary of Costs

Option	Total Costs ($)
0 – Do Nothing	N/A
1 – Preferred Option	$4.30 M (2017-2027)
2 – Defer [redacted]	$3.51 M (2017-2027)

6.4 Preferred Option Cost Breakdown

	17/18	18/19	19/20	20/21	21/22	22/23	23/24	24/25	25/26	26/27
Estimate ($M)	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		[redacted]	[redacted]
Total ($) 2017-2019	[redacted]									
Total ($) 2017-2027	[redacted]									

6.5 Summary of Risk

The preferred option addresses Reputation and Regulatory Compliance risks, as analysed utilising the 5x5 corporate risk matrix, as outlined in TasNetworks Risk Management Framework.

Risk Category	Risk	Impact	Likelihood	Consequence
Reputation	[redacted]	[redacted]	Unlikely	Moderate
Regulatory Compliance	[redacted]	[redacted]	Unlikely	Minor

The only risk to highlight for completion of this initiative is a potential for increased cost if the activities planned for 2017 period are not completed in time. This will have a financial and scheduling impact on other IT Security projects.

6.6 Economic analysis

Option No.	Option description	NPV	Reason got selection/rejection
0	Do nothing	$0	Infeasible
1	Preferred Option	-$2.96 M	
2	Upgrade existing platforms, but do not introduce new [redacted]		Risks not addressed, similar NPV to Preferred
3	Defer [redacted] and perform [redacted] during the determination period	-$2.42 M	Residual risk higher than Preferred for not much financial advantage

Further details of the NPV calculations can be found here:

IT.INF.08 NPV Calculations.xls

6.6.1 Quantitative Risk Analysis

N/A

6.6.2 Benchmarking

N/A

6.6.3 Expert findings

N/A

6.6.4 Assumptions

ITA-134	No major platform or architecture changes prior to 2017
ITA-135	[redacted]
ITA-136	[redacted]
ITA-137	[redacted]
ITA-138	[redacted]

Section 2 Approvals (Gated Investment Step 2)

Project Initiator:	[Enter name]	**Date:**	
Project Manager:	[Enter name]	**Date:**	

Actions			
Submitted for CIRT review:	[Enter date of CIRT here]	**Actioned by:**	[Enter name]
CIRT outcome:	[Enter details here] [Reference any minutes as appropriate.]		