Asset Management Plan

Corporate IT – Infrastructure

Record Number: R0000131777

Version Number: 1.0

Date: October 2015

Document Control

Authorisation

Action	Name and title	Date	Signature
Prepared by	Infrastructure Architect, Information Technology Group	24/06/2015	
Reviewed by	IT Infrastructure Team Leader		
Authorised by	Information Technology Leader		
Review cycle	2.5 Years from date of last approval		

Contact

This document is the responsibility of the Information Technology Group, Tasmanian Networks Pty Ltd, ABN 24 167 357 299 (hereafter referred to as "TasNetworks").

Please contact the Leader Information Technology with any queries or suggestions.

Responsibilities:

- Implementation — All TasNetworks staff and contractors.
- Compliance — All group managers.

Revision

Date	Version	Description	Author	Approved by
03/02/15	0.1	Draft Template	[redacted]	Draft
19/02/15	0.2	Initial Draft	[redacted]	Draft
24/03/15	0.3	Partial Draft for delivery to Finance	[redacted]	Draft
15/05/15	0.4	Incorporated feedback from [redacted]	[redacted]	Draft
24/06/15	0.5	Further content	[redacted]	Draft
13/10/15	0.6	Review and update	[redacted]	Draft
26/10/15	1.0	Issue 1.0 for purposes of redacting.	[redacted]	

Copyright

Table of Contents

1 Background and Purpose

The TasNetworks Information Technology team is responsible for delivering Architecture, Infrastructure and data network services; desktop services and application support; data management and development and project delivery, testing and governance. IT Infrastructure systems are the shared hardware, software, monitoring and administration tools forming the foundation of shared IT capabilities upon which business systems are built.

This Asset Management Plan details TasNetworks' plan for IT Infrastructure System assets for the 5 year period 2017 – 2022. The strategies outlined in this plan have been developed taking into account past asset performance, industry best practice and the need for prudent investment to optimise the asset lifecycle costs and performance.

The objective of this plan is to minimise business risk to within acceptable limits – utilising the TasNetworks risk framework and achieving reliable asset performance at an optimal lifecycle cost. The replacement program outlined will mitigate business risks presented by each asset category and optimise the economic life of each asset according to the important factors of inadequacy, supersession and obsolescence. These factors are relatively important when dealing with such complex technology, compared to wear and tear.

This plan supports the TasNetworks IT Strategy by providing effective and efficient solutions while rationalising the IT environment and reducing costs.

2 Scope

2.1 In Scope

This asset management plan covers the identification, procurement, implementation, maintenance and disposal of all IT Infrastructure systems within TasNetworks. IT Infrastructure systems include the following:

a) physical servers and hardware appliances;
b) shared storage solutions;
c) virtualisation technology;
d) enterprise backup system;
e) local area and wide area networking equipment;
f) core networks and perimeter (security) network equipment;
g) personal computing environment;
h) application delivery systems;
i) email, messaging and collaboration platform;
j) management and monitoring systems;
k) network access control;
l) identity management solution;
m) anti-malware and content filtering systems; and
n) intrusion detection and prevention systems.

2.2 Out of Scope

The following areas are not in the scope of this document, but are covered by their own Asset Management Plans:

- Business Support Services;
- Works & Service Delivery;
- Network Information Systems (NIS);
- Network Operation and Control System (NOCS); and
- Telecommunications Network Operation and Control System (TNOCS).

3 TasNetworks Asset Management

Investment drivers for IT Infrastructure stem primarily from the need to provide services that can maintain the required levels of reliability, efficiency, capacity, and supportability. Investment is required in order to maintain the currency and supportability of these systems and to cope with both realised and anticipated business growth. Investments in these projects are made to ensure that Corporate IT can continue to provide the required infrastructure to support business requirements.

IT equipment has a rapid rate of evolution, with vendors generally superseding products within 3-5 years. This change is partially driven by vendors updating their technology based on the availability of newer components (e.g. chipsets or CPUs), as well as through the implementation of entirely new technologies. The rapid shift in technologies limits the ability of suppliers and vendors to continue to maintain the older products, and as a result continued support for older products becomes increasingly expensive or unavailable.

In addition to the evolution in technology, demands on technology capacity are constantly increasing. As a result, older equipment often lacks the capability to deliver services required by the business.

Maintaining the IT infrastructure in a state that meets business requirements encompasses the activities and requirements documented in the following subsections.

Lifecycle Replacement

IT Infrastructure and associated software requires evaluation at the end of its expected life to determine any need for replacement in order to continue supporting business applications. End-of-life equipment no longer enjoys vendor support or maintenance, shifting all maintenance and support costs onto the owner. Additional drivers for lifecycle replacement include:

- Per-year warranty costs increase over the life of the asset;
- Per-instance patching and software upgrade costs increase over the life of the asset;
- The likelihood of software and hardware incompatibilities increases over the life of the asset;
- The number of servers each administrator can manage decreases as the servers become older;
- Baseline operating system performance degrades over time as the servers age;
- Hardware failure rates escalate after the third year in operation;
- In addition to the negative consequences listed above to delaying refresh cycles, new assets provide:
    - Reduced power and cooling costs;
    - Reduced administration costs;
    - Greater security and reliability; and
    - Smaller physical footprint (reduced demand for data centre space).

Capacity Management

The primary objective of Capacity Management activities is to ensure that IT capacity meets current and future business requirements in a cost-effective manner. Capacity Management activities include:

- Forward planning to identify and meet forecast growth and future business requirements;
- Installation, upgrade and replacement of platforms to meet forecast requirements; and
- Ongoing performance monitoring and management of IT systems.

Maintain Software Assurance

Corporate IT has a requirement to acquire and maintain software upgrade rights for all infrastructure related software licences and hardware firmware. These rights reduce support costs, allow maintenance of a high level of security and reduce upgrade costs through access to upgraded versions of software.

Software Assurance also guards against software bugs and potential vulnerabilities in out-of-date and superseded software versions.

Vendor Technical Support

Appropriate technical support agreements are required to deliver hardware and software support in a manner that meets IT service level requirements. Support requirements include:

- Fault diagnosis and resolution assistance;
- Software patches and updates;
- Firmware and BIOS patches and updates; and
- Hardware break fix support.

For critical systems, this support must be available 24 hours per day, 7 days per week in order to ensure the availability and effectiveness of infrastructure underpinning business application services. Complex systems will require vendor or manufacturer engineers to attend on-site to assist with fault resolution or perform scheduled maintenance activities.

Regulatory Compliance

While many of the items documented in this plan do not have direct regulatory implications, the infrastructure described does support the TasNetworks business in the execution of their regulatory responsibilities.

Two areas with direct regulatory implications have been identified, these are:

- TasNetworks backup and disaster recovery infrastructure supports TasNetworks ability to recover essential business services in the event of a disaster. These services enable the TasNetworks business to meet its regulatory requirements during a declared disaster.
- IT Security infrastructure directly supports TasNetworks efforts to ensure the privacy and protection of critical business assets and data. These efforts enable TasNetworks to meet data privacy and related regulatory compliance requirements.

3.1 Asset Management Influences

While not directly related to the management of IT assets at TasNetworks, the influences discussed briefly below will impact planning, implementation and lifecycle management processes and future strategy and purchasing decisions at TasNetworks.

Technology Trends

Relevant industry trends have been identified during the Determination process; these are discussed in the applicable asset class description sections that follow.

Transformative Technologies

The emergence of transformative technologies (also referred to as disruptive technologies or disruptive innovation) is a regular occurrence in the IT industry due to the rapid rate of technological change and massive ongoing spending in technology research and development. Once implemented and accepted, these technologies may result in significant changes to business processes, operating models and/or market conditions.

Past examples of transformative technologies in the IT industry include:

- The emergence of corporate computing in the 1960s;
- The development and acceptance of the personal computer in the workplace in the 1980s;
- The rapid growth and use if the internet from the late 1990s;
- The use of mobile devices and networks in the last decade; and
- The recent rise and popularity of cloud computing and infrastructure.

A number of disruptive technologies can be expected to emerge over the determination period, while some technologies currently in the early stages of adoption will gain widespread acceptance. Where applicable, both current and potential future disruptive technologies are discussed below.

By their nature, the budgetary impact of transformative technology adoption can be difficult to assess. Therefore in general a conservative approach to determination of both CAPEX and OPEX requirements in the Initiative Assessments within the scope of this plan has been taken.

4 IT Asset Class Description

IT assets include all hardware and software platforms required to deliver application and data access services to the TasNetworks business in a timely and effective manner. The assets listed below serve both 'live' production TasNetworks services as well as:

- Development and testing environments enabling enhancement of existing services as well as new services required by TasNetworks;
- IT Infrastructure Services delivered to Aurora Energy under the Transitional Services Agreement; and
- Provision of disaster recovery/business continuity capability to ensure continued access to data and applications.

Investment drivers for IT Assets stem primarily from the need to provide services to meet TasNetworks current and future availability and effectiveness. This investment is required in order to maintain currency and supportability of these systems and to cope with user demand, capacity growth and the evolving IT technology environment over the term of this asset management plan.

4.1 Server Hardware

This asset class refers to hardware infrastructure specifically designed for hosting of server applications, primarily (but not necessarily exclusively) in one or more of TasNetworks data centre facilities. Server hardware includes:

- Native Physical Servers: servers running a single operating system instance and one or more applications directly on the physical hardware and without an intervening virtualisation layer.
- Virtualisation Physical Servers: servers running virtualisation software, thereby hosting multiple logical operating instances on the hardware.

Server hardware includes the physical servers themselves as well as shared server infrastructure, required for blade server installations (including chassis, power supply and interconnect components).

As at mid-2015, TasNetworks operates [redacted].

Servers are typically operated to a [redacted] life cycle, while [redacted] components are refreshed less frequently [redacted]).

4.1.1 Technology Trends

Technology trends shaping server hardware include the following themes.

Server Virtualisation: server virtualisation can be defined as the partition of a physical server into multiple logical server instances. The benefits of virtualisation include:

1. Increased utilisation of server resources;
2. The ability of servers to survive failure of underlying hardware with minimal disruption to IT service delivery; and
3. Simplified IT backup and disaster recovery.

While this technology is now mature and ubiquitous, the capabilities provided by technology vendors continues to evolve to provide increased virtual server density, improved resilience and new functionality. Additionally, the previously dominant position of VMware in the server virtualisation

marketplace is being challenged by the increasingly capable Hyper-V virtualisation platform offered by Microsoft.

At TasNetworks, this trend is reflected in the planned program of work through:

- Continued expansion of the use of virtualisation technology to reduce the number of physical servers and subsequent capex investment;
- Continued upgrade of the virtualisation platform as new versions become available and mature;
- Review of the hypervisor platform in use at TasNetworks to determine long term platform selection; and
- Potential replacement of the hypervisor platform following the review.

Increasing Capacity: key server components continue to evolve to provide increased processing, memory and storage capacity. The 'scale out' of processors to include an increasing number of physical cores in the CPU footprint is both a driver and beneficiary of the trend towards server virtualisation, as is the increase in memory available to each server platform.

Windows Server: a new version of Windows Server will be released by Microsoft in early 2016. This release (tentatively titled Windows Server 10 or Windows Server 2016) will be supported by Microsoft well into the coming decade.

[redacted] However, over the length of the determination period the SOE [redacted] It is anticipated that update activities will be resourced from BAU operational support activities and that major application platforms will be updated to the new SOE when major version upgrades take place.

Linux: the Linux operating system has been widely adopted in the marketplace, although largely for specialist applications with relatively few organisations adopting the platform for general server operations. More extensive adoption of the platform is hindered by a number of issues (both real and perceived), including:

- The requirement for widely used Microsoft enterprise server software to be hosted on Microsoft Windows server operating systems;
- Perceived lack of support (although enterprise-grade support is provided by major vendors, such as Red Hat and SUSE); and
- Perceptions regarding the enterprise-readiness of 'free'/GPL-licensed software.

[redacted]
Although there are no plans for general adoption of Linux in the determination period, it remains an option for selected applications where there are clear and tangible benefits associated with its use. Any installations will be accompanied by support and maintenance agreements appropriate to the service delivered from the platform or platforms.

4.1.2 Transformative Technologies

The transformative technologies described below will be regularly evaluated by TasNetworks IT to determine the benefits and risks of implementation. Implementation of the technologies will take place as recommended by review activities:

Cloud Computing: As a logical extension of both the virtualisation of server workloads and the commoditisation of underlying hardware, cloud computing (in all of its forms) is a rapidly maturing IT technology. The use of cloud software, platform and infrastructure services is anticipated by TasNetworks in order to:

1. Allow rapid development and deployment of application services;
2. Provide temporary 'burst' capacity;
3. Allow deployment of new application services available only as cloud applications; and
4. Reduce capital expenditure on IT infrastructure.

The identification, approval and implementation of cloud computing at TasNetworks will be influenced by a number of considerations, including:

- Regulatory requirements regarding data security, integrity and sovereignty;
- Availability of local providers, including provision of services by TasNetworks non-prescribed business units;
- Availability and suitability of applications delivered under the software-as-a-service (SaaS) model;
- Stability (both technical and financial) of cloud service providers; and
- Financial impacts.

DevOps: DevOps (a portmanteau of *Development* and *Operations*) aims to bridging the gap between projects and operations by using Agile techniques both in development, project management and system administration activities. Of particular interest to IT infrastructure management is the use of 'configuration as code' techniques to automate the deployment, management and maintenance of IT server infrastructure.

Implementation of DevOps technologies and processes has great potential to improve both the quality and efficiency of IT operations by automating many tasks traditionally carried out by IT operations support staff. TasNetworks' recent implementation of [redacted] provides a platform from which the benefits of this technology can be realised. It is anticipated that this platform will be increasingly utilised to improve the reliability, manageability and effectiveness of IT operations in an evolving and increasingly complex environment.

Converged Infrastructure: Converged infrastructure operates by grouping disparate IT components into a single, optimised computing package. Components of a converged infrastructure may include servers, data storage devices, networking equipment and software for IT infrastructure management, automation and orchestration. Converged infrastructure can take two forms:

1. 'Traditional' converged infrastructure, where the infrastructure is constructed from components according to a validated architecture. Each of the components in the infrastructure is a discrete component that can be also used for its intended purpose.
2. 'Hyper-converged' infrastructure, where components are tightly integrated and software defined. The technology is integrated to the point where it cannot be broken out into its constituent components.

A converged infrastructure addresses the problem of siloed architectures and IT sprawl by pooling and sharing IT resources. Rather than dedicating a set of resources to a particular computing technology, application or line of business, converged infrastructure creates a pool of virtualised server, storage and networking capacity that is shared by multiple applications and lines of business.

Through the existing use of server and storage virtualisation, TasNetworks is already on the path to converged infrastructure. Future activities will assess the benefits, opportunities and risks of further convergence (including the introduction of hyper-converged platforms) to reduce the costs associated with both implementation and ongoing operation of IT infrastructure, as well as increase the agility of IT operations.

4.2 Storage Hardware

For the purposes of this document, storage hardware refers specifically to infrastructure installed to provide shared storage for servers and server applications as well as general document storage. Storage hardware includes:

- Storage Area Network (SAN) and Network Attached Storage (NAS) infrastructure;
- [redacted]

[redacted] Storage hardware of this type is typically operated on [redacted] life cycle as it is considered mid-range. Annual maintenance and support charges for such arrays are significantly increased [redacted] to send a strong price signal to customers to upgrade and replace.

4.2.1 Technology Trends

Technology trends influencing storage hardware operations include the following themes.

Increasing Demands for Storage: while not specifically a storage technology trend, new application technologies and services are driving an increasing demand for storage capacity. These services include:

- Big Data and massive-scale data warehousing;
- Ubiquitous device connectivity and instrumentation; and
- Increasing use and storage of rich media, including high quality video streams.

The increased volume and diversity of data being stored and new requirements to index, search and analyse this data result in a growing reliance on storage resource management tools to limit the operational overheads accompanying storage growth. This in turn places additional costs on storage acquisition and storage management software licensing.

Increasing Storage Capacity and Density: Fortunately (in light of increasing demands for storage discussed above), storage capacity and density continues to increase. Magnetic disk drives are now commonly sold in capacities of 1.8TB each, while 'near line' magnetic disk drives with 6TB capacity are now available.

Increased Storage Performance: The explosive growth of Solid State Disk (SSD) technologies has enabled a tremendous increase in the performance of data storage platforms. While earlier generations of the technology lacked capacity, reliability or back-end storage bus performance, the technology is now widely deployed across the IT industry.

Relieving or removing performance bottlenecks associated with disk performance does however present new challenges, both in the storage systems themselves (which generally require redesign to take advantage of disk performance) and in overall systems Implementation and management operations

(relieving storage bottlenecks often exposes performance constraints in other areas of the system architecture).

4.2.2 Transformative Technologies

'Big Data': Big Data is a broad term for data sets so large or complex that traditional data processing applications are inadequate. Challenges include analysis, capture, search, sharing, storage, transfer, visualisation, and information privacy. The term can also refer to the use of predictive analytics or other advanced methods to extract value from data.

Analysis of data sets can find new correlations unavailable to traditional data processing methods. IT departments across most industry sectors are encountering with large data sets in areas including Internet search, finance and business informatics.

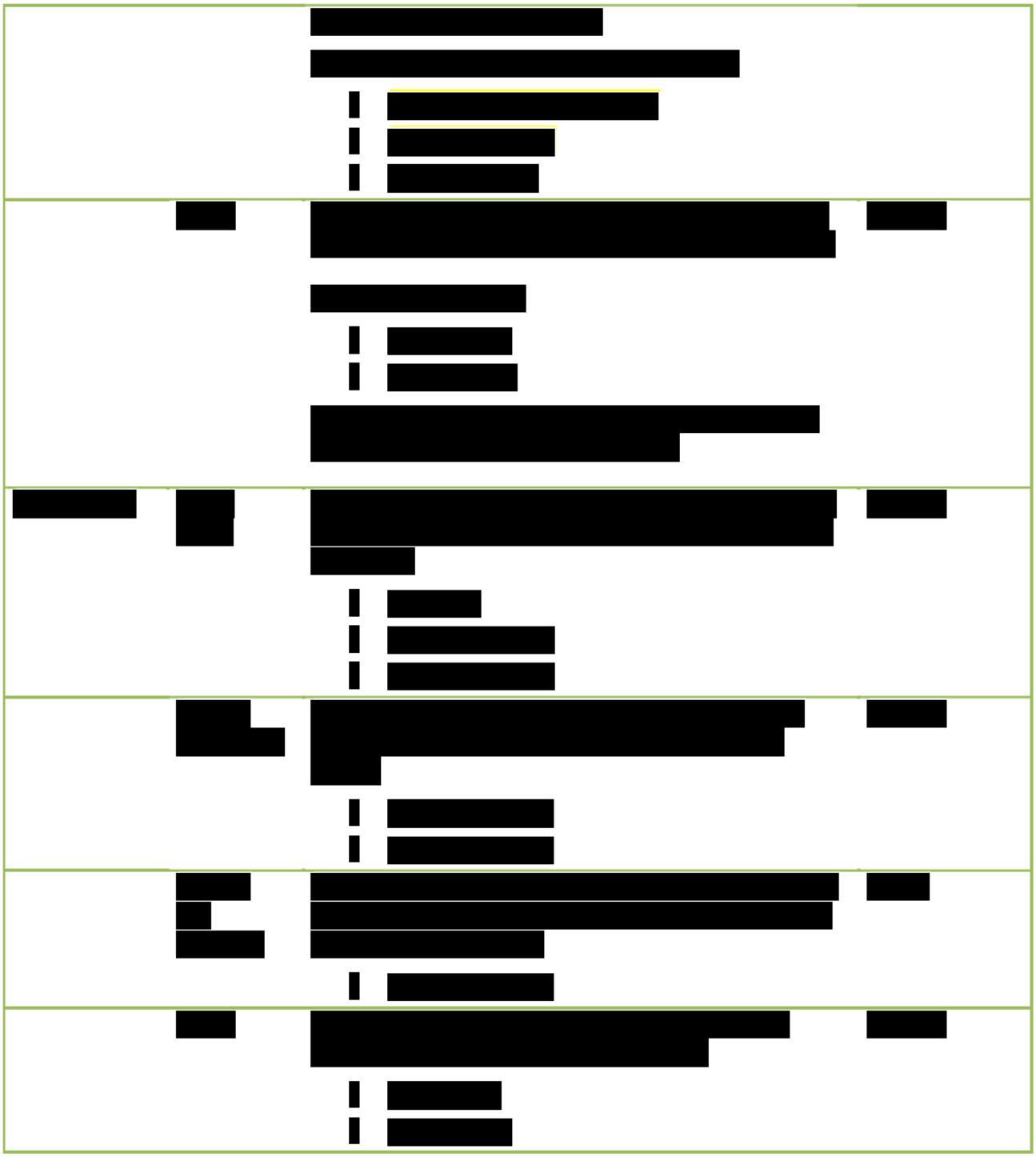
Data sets grow in size in part because they are increasingly being gathered by cheap and numerous information-sensing mobile devices, aerial (remote sensing), software logs, cameras, microphones, radio-frequency identification (RFID) readers, and wireless sensor networks. Relational database management systems and desktop statistics and visualisation packages often have difficulty processing these data sets. The work instead requires "massively parallel" software running on tens, hundreds, or even thousands of servers.

Given the nature of TasNetworks business, including the potential future use of sensor and drone technologies to monitor the state of the transmission and distribution, this technology is likely to have an impact on data processing and storage operations. Adoption of the technology will require new approaches to systems design and the adoption of platforms and products to match.

Convergence and Hyper-Convergence: Discussed above, converged infrastructure technologies will have a major impact on storage architecture and administration at TasNetworks if adopted. In many ways the convergence of infrastructure represents a return to the previous mode of operation, before the widespread adoption of shared storage technology, however today's application environment will require careful consideration regarding how and where converged infrastructure can be successfully deployed at TasNetworks.

4.3 Network Infrastructure

Location	Hardware Type	Description/Notes	Typical Lifespan
[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]



The Infrastructure team is responsible for the operation and periodic replacement of approximately [redacted] such devices across Tasmania.

4.3.1 Technology Trends

The network technology trends discussed below have been considered when planning the program of work for the determination period.

Internet Protocol Version 6 (IPv6): Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is intended to replace IPv4 [1].

IPv6 adoption is considered essential to the long-term operation of TasNetworks network infrastructure and dependent services. Support for (or at the very least interoperability with) the protocol is currently a requirement for all hardware and software implemented. A formal program to transition the TasNetworks LAN/WAN infrastructure to IPv6 is included in the estimates for the LAN Refresh and Network Management Investment Evaluation Summary (IT.INF.03).

[redacted]

Use of 40 and 100 gigabit Ethernet technologies brings the following benefits to the data centre:

- Increased data communications bandwidth to support increasing requirements for data transmission and storage;
- Increased efficiency of single high-capacity connections as opposed to aggregation of multiple physical links; and
- Increased efficiency of fibre optic communications through reduction in the number of optical frequencies required for high-bandwidth transmission of data.

[redacted]

[1] http://en.wikipedia.org/wiki/IPv6

[redacted]

Software Defined Networking: Software Defined Networking (SDN) is an approach to computer networking that allows network administrators to manage network services through abstraction of functionality. This is done by decoupling the system that makes decisions about where traffic is sent (the control plane) from the underlying systems that forward traffic to the selected destination (the data plane).[2]

Advantages claimed by proponents of SDN include:

- Directly programmable: Network control is directly programmable because it is decoupled from forwarding functions;
- Agile: Abstracting control from forwarding lets administrators dynamically adjust network-wide traffic flow to meet changing needs;
- Centrally managed: Network intelligence is (logically) centralised in software-based SDN controllers that maintain a global view of the network, which appears to applications and policy engines as a single, logical switch;
- Programmatically configured: SDN lets network managers configure, manage, secure and optimize network resources very quickly via dynamic, automated SDN programs. The programs are easily written because they do not depend on proprietary software; and
- Open standards based and vendor neutral: When implemented through open standards, SDN simplifies network design and operation because instructions are provided by SDN controllers instead of multiple, vendor-specific devices and protocols.

[redacted] These platforms will be evaluated as part of data centre LAN refresh activities, with adoption considered likely.

4.3.2 Transformative Technologies

Cloud Computing: Discussed above, the widespread deployment of Software, Platform and Infrastructure-as-a-Service computing will place an increasing reliance on the availability and performance of WAN interconnects and internet connectivity.

National Broadband Network: Ongoing rollout of the National Broadband Network provides TasNetworks with additional options to improve available bandwidth to remote site locations in a more cost-effective manner than has been historically available. Increased available communications capacity can potentially allow additional services to be deployed to these locations, including (but not limited to):

- Audio and video conferencing;

[2] http://en.wikipedia.org/wiki/Software-defined_networking

- Video recording for site and asset monitoring and maintenance activities.

Additionally, the NBN rollout will drive new opportunities for business-business (B2B) and business-customer (B2C) engagement through the deployment of new application services with high data communications capacity requirements.

Finally, staff access to high-speed internet connectivity will provide increasing scope for deployment of remote access to TasNetworks application services and potentially reduce required travel time (and associated Occupational Health and Safety risks).

4.4 Client Hardware

Client hardware includes all endpoint devices connecting to the TasNetworks network infrastructure and accessing TasNetworks data and/or applications (with the exception of mobile phones). This hardware includes:

- Desktop computers;
- Laptops and notebooks; and
- [redacted]

For the purposes of this document, 'client hardware' specifically excludes mobile phones and other tablets (although they may access TasNetworks mail and scheduling application, they do so from outside the TasNetworks LAN/WAN). The definition also includes network-connected printers and multifunction devices.

The table below lists the types and number of client devices supported by TasNetworks IT as at mid-2015.

Type	Quantity	Typical Lifespan
Desktop Computers	[redacted]	[redacted]
Laptop/Notebook Computers	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

4.4.1 Technology Trends

Mobile Devices: The use of tablet and mobile phone platforms to access enterprise application and data services is becoming increasingly important to enterprises. Use cases are no longer confined to relatively simple mail and calendar access as mobile devices connect to core business applications. The impacts of this trend include:

- Requirements to manage and secure mobile devices accessing corporate networks;
- The need to modify application presentation to enable mobile device access; and
- Demand for appropriately connected wireless LAN services.

TasNetworks anticipates widespread adoption of these devices for production usage leading to and during the determination period. Activities to facilitate this adoption (including Mobile Device Management (MDM) platforms and continued provision and upgrade of wireless LAN services) have been included in the proposed program of work [redacted]

Windows 10: Windows 8.x adoption rates remain low in the enterprise; most organisations are waiting for the release of Windows 10 in Q3/2015 to provide an upgrade path from Windows 7 on desktop operating systems. Windows 10 will provide significant improvements over 8.x, particularly for corporate and enterprise users.

A notable feature of the coming operating system release is the use of a single code base for desktop and mobile form factor devices. In theory, this will greatly simplify the management of endpoint devices (provided of course that Windows 10 tablets and handsets are the chosen enterprise mobile device).

TasNetworks next desktop SOE refresh [redacted]

Office 16: The next version of Microsoft's office productivity software (Office 2016) will be released in the second half of 2015. [redacted]

4.4.2 Transformative Technologies

Desktop Virtualisation: Desktop Virtualisation technologies (also known as Virtual Desktop Infrastructure or VDI) separate the desktop and application processing hardware from access devices. Typically, desktop and application services are hosted in the data centre on server hardware and accessed by the user using client software installed on a PC/laptop, tablet/phone or dedicated thin-client device.

Implementation of desktop virtualisation brings a number of advantages, including:

- Potential to defer desktop upgrades, as endpoint computing capacity is no longer relevant to desktop and application performance;
- User experience portability, where the user accesses the same desktop regardless of location or connecting device;
- Increased security through centralised hosting and control of desktop services; and
- Increased flexibility, enabling SOE and operating system upgrades to take place with considerably less complexity and effort.

[redacted]

Bring Your Own Device (BYOD): BYOD refers to the policy of allowing employees to use personal devices to access corporate networks, applications and data. While in the past such a policy would often be rendered unworkable due to device security and management concerns, the widespread adoption of VDI technologies (as discussed above) allows corporate desktop environments to be accessed from these devices while remaining hosted and controlled by Corporate IT.

Adoption of BYOD will require changes to corporate and IT policies as well as implementation of appropriate technical controls. The feasibility of adoption will be assessed in conjunction with the VDI assessment discussed above.

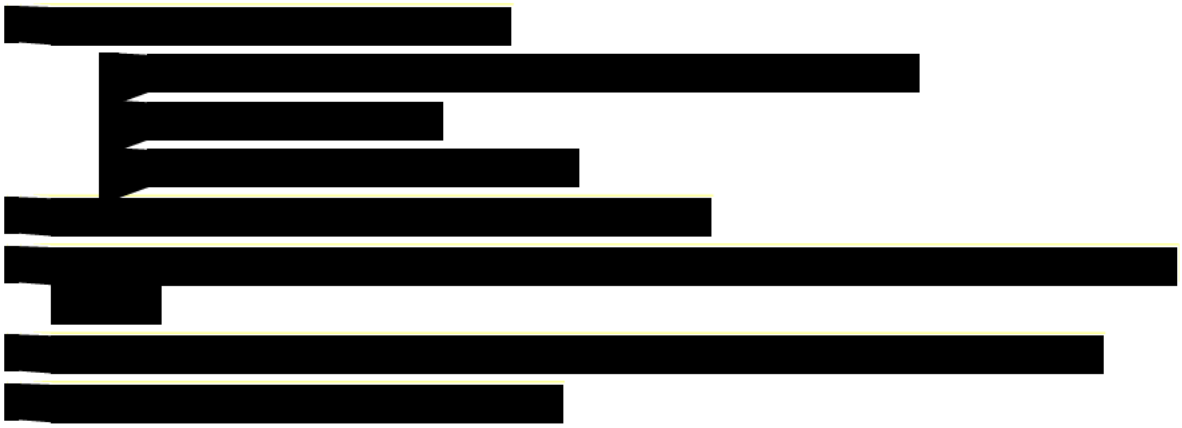
4.5 Security Hardware and Software

Investment drivers for security systems stem primarily from the need to provide services that can maintain reliability, efficiency, capacity and supportability. The investment is needed to maintain currency and supportability of these systems and to cope with user demand, performance as well as the evolving security environment and threat requirements over the term of the asset management plan.

The high-level strategic objectives of IT security systems are to:

- 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;
- Detect and respond to security incidents in order to correct damage and evaluate incidents that have occurred; and
- Effectively respond to security incidents.

The scope of installed security platforms includes:



4.5.1 Technology Trends

Evolving Threat Landscape: Threats to IT systems and data are rapidly evolving in complexity and capability. As the European Union Agency for Network and Information Security (ENISA) states:

'No previous threat landscape document published by the European Union Agency for ENISA has shown such a wide range of change as the one of the year 2014. We were able to see impressive changes in top threats, increased complexity of attacks, successful internationally coordinated operations of law enforcement and security vendors, but also successful attacks on vital security functions of the internet.'[3]

In addition to the increasing sophistication of attacks by criminal organisations, unfriendly nation-states and non-state actors (both terrorist and activist organisations), many of the technology trends described elsewhere in this document enable new vectors for compromise of IT systems and data. Examples include:

- Increasing use of mobile devices in the enterprise;
- Adoption of cloud computing; and
- Interconnected devices.

In order to avoid or mitigate the technical, financial and reputational impact of security breaches, TasNetworks will continue to implement, upgrade and maintain security platforms as outlined in the IT Security Investment Evaluation Summary. Additionally, the need to maintain the security and integrity of

[3] ENISA Threat Landscape for 2014

IT systems is a driver for many of the infrastructure upgrade and replacement activities documented in other Investment Evaluation Summaries.

4.6 [redacted]

[redacted]

- [redacted]
- Desktop productivity applications:
  - [redacted]
- Server applications:
  - [redacted]
- IT Service Management applications:
  - [redacted]

[redacted]

Type	Examples and Notes
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

4.6.1 Technology Trends

Technology trends regarding server and client software are discussed in the respective preceding sections of this document.

4.6.2 Transformative Technologies

[redacted]

4.7 Other Server and Client Software

[redacted]

4.7.1 Technology Trends

Software as a Service (SaaS): many vendors are now offering software services as a service offering hosted externally to the customer (either on vendor infrastructure or increasingly over major infrastructure service providers). This architecture has matured to the point where it is the preferred service delivery model for many software vendors.

Use of SaaS offerings offers particular attractions for services where specialised support skills are difficult and/or expensive to acquire and maintain, or are considered outside the scope of services that reasonably can be provisioned and supported by in-house IT departments. In these cases, use of SaaS offerings can allow deployment of these application services under circumstances where they would otherwise be not practical.

As with all cloud computing services, care and attention needs to be paid to maintaining the security and integrity of TasNetworks data. An additional complication to be addressed is the impact of these services on operational budgets where previously it was preferable to favour development capital assets.

4.7.2 Transformative Technologies

Hosted and Service-Based Data Analytics: also known as Big Data as a Service (BDaS), these services leverage the massive amounts of compute and storage capacity available in public IT service provider infrastructure to provide large scale data analysis services with little or no need for expensive on-premises infrastructure. These services can often integrate other public and private data services into the analytics process (for example geospatial and social networking data) that would not otherwise be available.

These services are particularly useful for processing large data sets where the data processed is of low business sensitivity, but as always caution is advised for more sensitive data, including referencing data privacy, integrity and sovereignty requirements before adoption.

5 Asset Maintenance & Lifecycle

During the first year of operation since the merger, TasNetworks embarked on a programme to implement a fully-integrated in-house IT Service Desk model. The TasNetworks IT Infrastructure Team is responsible for the management, implementation and support of all the system assets discussed in this Asset Management Plan. A summary of general lifecycle reviews/dates is shown in the following table.

Asset	Event	Timeframe	Driver
			To adequately support business and operational IT systems through the provision of reliable and fit for purpose IT infrastructure. Replace equipment within a

			suitable economic lifespan, maintaining active vendor warranty support to facilitate timely remediation of any hardware faults.
[redacted]	[redacted]	[redacted]	As above
[redacted]	[redacted]	[redacted]	As above
[redacted]	[redacted]	[redacted]	As above
[redacted]	[redacted]	[redacted]	As above
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	Maintain current supported OS and core applications
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	Maintain current supported application versions
[redacted]	[redacted]	[redacted]	Maintain current supported application versions
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	Maintain current supported application versions. Maintain up to date security controls to keep up with evolving threat landscape.
[redacted]	[redacted]	[redacted]	As above
[redacted]	[redacted]	[redacted]	As above
[redacted]	[redacted]	[redacted]	As above

	[redacted]		
[redacted]	[redacted]	[redacted]	As above
[redacted]	[redacted]	[redacted]	Replace equipment within a suitable economic lifespan. Maintain up to date security controls to keep up with evolving threat landscape.

Table 1 – Planned Asset Upgrades

5.1 Condition Monitoring Practices

TasNetworks has adopted a strategy of implementing both proactive and reactive condition monitoring of IT assets, including physical, virtual and software assets.

The goal of proactive monitoring is to predict likely incidents with sufficient notice and actionable alert information to enable IT staff to take corrective action and avoid any system outages.

Reactive monitoring aims to detect incidents affecting IT assets as quickly as possible during or after they occur, to capture sufficient information for the incident to be rectified as quickly as possible.

TasNetworks operates several systems to monitor the infrastructure discussed here, largely centred on [redacted] Where the functionality of [redacted] is not sufficient with regard to particular infrastructure assets or systems, other monitoring and management systems are used; e.g. [redacted]

5.2 Defect Management

Infrastructure defects are managed through the Service Request, Incident and Problem Management processes and implemented within the IT Service Management tool. A key component of this system and these processes is the front line Service Desk, who field telephone calls and email requests. The Service Desk escalates calls to the Infrastructure Team, as well as incidents or tickets being raised by the alerting and monitoring systems directly.

6 TasNetworks Issues and Opportunities

6.1 Current Issues (Mid 2015)

6.1.1 Asset Issues

The most widespread issue facing the infrastructure assets in the scope of this plan is the age of operating systems running on servers. This is a difficult challenge to address as it relies on the systems and software being compatible with current operating systems. While deploying a new set of servers with a current operating system is relatively straightforward, it is often a difficult and complex undertaking to upgrade or redeploy the software application itself, particularly if the application has been modified or customised.

The other general pressure on infrastructure assets is the continuing increase in requirements for more storage, more computing power and better network bandwidth.

6.1.2 Asset Condition Summary

6.2 Strategies & Opportunities

6.2.1 Servers and Storage

As outlined elsewhere and also considered within the relevant Investment Evaluation Summaries, the emerging technologies of hyper-convergence (combining servers, storage and backups into one device) and software defined storage should be investigated in light of the various claims made about these technologies. Chief among the claims is that they can be more cost effective than traditional approaches.

6.2.2 Mobility

Significant effort is being made already to address the needs of an increasingly tech-savvy workforce. Employees expect to be able to use mobile devices, including their own personal devices, to access systems at any time. Projects are already underway to improve and extend existing systems to deal with mobile device management, and the delivery of applications in a flexible and powerful way. These efforts are reflected in various points throughout the infrastructure initiatives, chiefly in IT.INF.06 – Application Delivery.

6.2.3 Network and Security

Network equipment has the longest lifecycle of any of the assets in scope of this plan, and is the most mature technology. There are several activities planned in this area, primarily to keep pace with the evolving threat landscape.

7 Initiatives

The following initiatives were categorised using the TasNetworks Technology Reference Model as a guide. Each initiative may represent several distinct projects across the determination period. These projects have been costed and grouped into the following eight initiatives.

7.1 Infrastructure Hardware

Infrastructure hardware initiatives include maintenance, upgrade and replacement activities for servers, storage and backup infrastructure.

Initiative ID	Summary	Estimated / Required Delivery
IT.INF.01	Server Refresh and Virtualisation Platform	[redacted]
IT.INF.02	Storage Refresh and Backup Review	[redacted]

Table 2 – Initiative Summaries

7.2 Data Networking

Data networking initiatives include maintenance, upgrade and replacement activities for both datacenter and end-user network infrastructure, but excluding network security platforms described below.

Initiative ID	Summary	Estimated / Required Delivery
IT.INF.03	LAN Refresh and Network Management	[redacted]
IT.INF.04	WAN Services	[redacted]

Table 3 – Initiative Summaries

7.3 Personal Computing Platform

Personal computing platforms include desktop, laptop and field worker Motion Tablet hardware, as well as the software standard operating environment (SOE) for these devices. In conjunction with the hardware assets, the systems used to deliver applications to those devices are considered in the Application Delivery initiative which considers the demands of an increasingly mobile and tech-savvy workforce. Applications are expected to be delivered seamlessly on a range of devices from a range of locations. Please note that a large proportion of software licensing is documented in Platform Software or elsewhere within the determination streams.

Initiative ID	Summary	Estimated / Required Delivery
IT.INF.05	Desktop and Laptop Fleet	[redacted]
IT.INF.06	Application Delivery	[redacted]

Table 4 – Initiative Summaries

7.4 Platform Software

Platform software includes operating system, application and operations management software licensed under TasNetworks Microsoft Enterprise Agreement as well as system and utility software licenses obtained from other vendors (such as Citrix, Oracle and McAfee).

Initiative ID	Summary	Estimated / Required Delivery
IT.INF.07	Platform Software	[redacted]

Table 5 – Initiative Summaries

7.5 [redacted]

Initiatives documented in the [redacted] account for anticipated maintenance, review, upgrade [redacted]

Initiative ID	Summary	Estimated / Required Delivery
IT.INF.08	[redacted]	[redacted]

Table 6 – Initiative Summaries

8 Program of Work

8.1 Project Definition and Selection

The initiatives have been prioritised on the basis of several key factors:

- Level of dependence of other systems (e.g. quality of shared storage has a large impact on many other aspects of IT systems);
- Level of flexibility with regard to scope or cost (e.g. software licensing costs are essentially unavoidable, unless systems are decommissioned altogether); and
- Variability of scope (some initiatives have elements of their scope which could conceivably be reduced, whereas other initiatives are effectively all or nothing).

8.2 Priority List

Priority	Initiative ID	Summary	Est/Req Delivery	Estimated Cost
Must have 1	IT.INF.07	Platform Software	[redacted]	$5.9M
Must have 1	IT.INF.04	WAN Services	[redacted]	$3.2M
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Must have 2	IT.INF.02	Storage Refresh and Backup Review	[redacted]	$7.5M
Must have 2	IT.INF.01	Server Refresh and Virtualisation Platform	[redacted]	$3.3M
Must have 2	IT.INF.03	LAN Refresh and Network Management	[redacted]	$4.0M
Need to have 1	IT.INF.05	Desktop and Laptop Fleet	[redacted]	$4.5M
Like to have 1	IT.INF.06	Application Delivery	[redacted]	$3.3M

Table 7 – Initiative Priorities