Asset Management Plan

Corporate IT – Software Asset Management Plan

Record Number: R0002349599

Version Number: 2.0

Date: November 2022

Authorisations

Action	Name and title	Date
Prepared by		15/11/2022
Reviewed by		19/12/2022
Authorised by		
Review cycle	5 Years from date of last approval	

Responsibilities

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 Head of Digital Solutions with any queries or suggestions.

Responsibilities:

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

Disclaimer

Reference documents

R954721 – TasNetworks Strategic Asset Management Plan

R40766 – TasNetworks Asset Management Policy

R909655 – TasNetworks Risk Management Framework

Record of revisions

Revision	Details	Date
1.0	Document updated for R19	27/10/2017
2.0	Major update incorporating R24	22/12/2024

Table of contents

List of Figures

List of Tables

1 Glossary

Table 1 - Document glossary

Term	Definition
ADM	Architecture Development Method. A detailed, step-by-step method on how to develop enterprise architecture by TOGAF.
AEMO	Australian Energy Market Operator. Delivers an array of gas and electricity market, operational, development and planning functions.
AMP	Asset Management Plan
CAPEX	Capital Expenditure
COTS	Commercial off the shelf. Usually refers to ready-made packaged software that can be deployed with configuration rather than customisation.
DNSP	Distribution Network Service Provider
EDW	Enterprise Data Warehouse. A central data repository of key business information assets that can be used for integration, reporting, data-mining and business intelligence.
EIM	Enterprise Information Management
ERP	Enterprise Resource Planning system
EWR	Electrical Works Request
GPS	Global Positioning System
HSEQ	Health, safety, environment and quality management
IT	Information Technology, inclusive of Digital Technology. In this document, the terms IT and Digital are used interchangeably.
ICT	Information and Communication Technology. This is an industry standard term to recognise the broad range of technologies covering computers, software, mobile and communication devices.
Investment Evaluation Summary (IES)	IES is an investment case articulating the investment reason, business benefits, risks, options considered, NPV and alignment with business strategy
MC	Metering Contestability
MDP	Metering Data Provider
MDMS	Meter Data Management System
MPB	Metering Provider Type B
NECF	National Energy Customer Framework

Term	Definition
NEL	National Electricity Law
NEM	National Electricity Market
NER	National Electricity Rules
NOCS	Network Operation and Control System
OPEX	Operating Expenditure
OT	Operational Technology is technology that is able to cause change (supervisory control) or detect change (data acquisition) regarding physical devices.
OTTER	Office of the Tasmanian Economic Regulator
POW	Program of Work
RCP	Regulatory Control Period
R24	Revenue Reset July 2019 to June 2024.
R29	Revenue Reset July 2029 to June 2034.
SaaS	Software-as-a-Service. A software delivery and licensing model that leverages the advantages of cloud computing.
SAM	Strategic Asset Management business division
TESI	Tasmanian Electricity Supply Industry.
TNOCS	Telecommunications Network Operation and Control System
TOGAF	The Open Group Architecture Framework

2 Background and Purpose

Around the world, electricity systems are undergoing fundamental change. At the heart of the change are electricity customers. Across Australia, these customers want more choice and control over their energy use, more renewable energy, lower costs and high levels of electricity system security and reliability.

As the owner and operator of the electricity transmission and distribution systems in Tasmania, TasNetworks is planning its future in this world of change. We are planning how we will continue to serve our customers into the future, and achieve our vision to be 'trusted by our customers to deliver today and create a better tomorrow'.

Customer benefit is the key driver for the investments we make. We must also ensure our network is safe, reliable and complies with a range of compliance obligations. We are working hard to keep our costs and our prices as low as we sustainably can, while delivering safe and reliable services.

For Digital Technology to deliver sustainable value it must support and enable TasNetworks to achieve its strategic business goals: safety; resilience; efficiency; renewable energy; and growth. TasNetworks has outlined five Digital Strategy goals that align to TasNetworks corporate goals:

- **Simple to use:** Empowering our field work force with simple to use and automated solutions;
- **Back to our core:** Support flexible, lean and commercial customer and network delivery;
- **Digital first:** Making digital the way we work, developing a future fit digital workforce;
- **Data driven:** Enable fit for purpose and data driven asset decisions;
- **Security by design:** Minimise risk to our people, assets and operations.

The Digital Services and Solutions Group is responsible for managing a broad range of corporate information technology services, from desktop and application support to the development and management of specialised business applications and technological capabilities that support core business operations for the enterprise. The Digital Group is also in charge of formulating a Digital strategy that builds on existing strengths and supports TasNetworks' strategy roadmap, thus meeting the future needs of the business.

TasNetworks actions its philosophy for asset management through asset management plans (AMP). These documents separate the infrastructure into subsets of like assets with a plan in place for each subset. This Asset Management Plan is concerned with TasNetworks' corporate Digital software solution assets.

The strategies included in this AMP have been developed taking into account past asset performance, industry best practices and the need for prudent investment to optimise cost and asset performance. These strategies also align to TasNetworks' business strategic goals outlined above.

2.1 Purpose of this plan

The purpose of this document is to support the TasNetworks 2024-2029 Combined Proposal, and to contribute to the achievement of the company's business strategic objectives outlined above. This document makes up part of the overall Combined Proposal that contains details of the TasNetworks corporate Digital software assets, the proposed forecast capital expenditure on these assets, expressed in 2021/2022 dollar terms, and the methodology used in developing the program of work.

This document should be read in conjunction with other relevant documents supporting the submission. Supporting documentation further establishes the background, justification, benefits, prudency and prioritisation of the investment decisions covered in this document.

2.2 Benefits of Digital Investment

In order for the enterprise IT environment to support and drive the organisational strategic goals, it needs to undergo a significant transformation. The initiatives identified by this plan have been carefully selected to enable and support business goals and to deliver on a range of benefits, including:

- Deliver a range of new and enhanced services to TasNetworks' customers that will help them better manage and control their electricity costs, provide additional communication channels and deliver a range of other services and information that they value;
- Ensure TasNetworks avoids significant risks associated with the end-of-life of related applications, some of which will be unsupported prior to 2029;
- Provide systems, processes and tools to support the introduction of cost-reflective tariffs and the roll-out of advanced meters, enabling customers to better control their energy use and manage peak demand;
- Enable TasNetworks to meet its regulatory and customer obligations in a prudent and efficient way, by delivering efficiencies in the core areas of the business and avoiding the additional expenditure associated with manual processes;
- Minimise threats to security and privacy of personal information that TasNetworks is required to keep in relation to its customers, contractors and employees;
- Empower TasNetworks staff, customers and partners to capture, access and share accurate information when they need it, wherever they may be;

- Enable customers and business to derive maximum value from our increased information collection for improved decision making and reporting;
- Maximise the value from our enterprise platform (ERP) investment by further integrating business solutions within the environment and aligning access to it. This will enhance team members mobility and productivity, allowing TasNetworks to cost effectively respond to external changes;
- Enable TasNetworks to maintain reliability and quality of Digital services, in line with agreed service level targets and future business, customer and regulatory requirements;
- Enable TasNetworks to control and, where possible, reduce technology costs in the long term through operational improvements, consolidation of Digital applications and improved governance;
- Empower TasNetworks staff to better leverage improved data access and quality through the adoption of advanced technology and further consolidation of systems, optimising flow of information for operational purposes and supporting the understanding of customer needs;
- Enable the long-term convergence of Information Technology (IT) and Operational Technology (OT) through the continual review and alignment of Technology led projects to the 2030 strategy roadmap and Enterprise Architecture evolution.

2.3 Challenges in the management of Digital software assets

TasNetworks Digital group face a number of challenges with its software asset base. Corporate software assets have significantly shorter lifespans than other corporate assets. Worse still, these lifecycles are often forced even shorter by rapidly evolving technology and business requirements. Many software systems must be regularly maintained or possibly replaced just to meet business, market, functional and performance requirements. Meanwhile, emerging technologies and bodies of knowledge are driving the need for much greater integration of data and functionality between systems including comprehensive business intelligence. The following list summarises the key asset issues:

- Rapidly evolving business and market requirements are driving significant demand on stretched resources and make long-term forward planning of software projects challenging;
- Ongoing evolution of underlying technologies require regular reassessment of TasNetworks' Digital architecture;
- Visibility of software vendor roadmaps is often difficult to achieve, making advance planning more difficult. Sometimes TasNetworks has little choice but to implement upgrade or replacement projects when vendors change their product offerings;
- Increasing reliance on IT systems and growing trends in business intelligence and big data are resulting in rapidly increasing demands on TasNetworks IT infrastructure. It is an ongoing challenge to maintain an appropriate capacity in terms of servers, CPUs, memory and storage;
- A rapid increase in the need to integrate disparate systems has led to an exponential increase in system interdependencies, increasing the complexity of managing TasNetworks' software assets;
- Limited internal resourcing results in greater utilisation of external resources, which impacts both costs and retention of intellectual property;
- Limited availability of skilled resources to hire or engage on a short-term basis, can prevent TasNetworks from commencing some projects or require the project to be significantly delayed;

- When national bodies change protocols and procedures TasNetworks is obligated to follow to operate in the National Electricity Market, TasNetworks is obliged to implement the changes in order to remain compliant to regulations.

3 Scope

3.1 In Scope

This asset management plan (AMP) covers the rationale for Corporate IT initiatives identified for the 2024-20 regulatory control period.

This AMP does not cover the management of all software assets at TasNetworks. This document details the management plans for enterprise and business support IT software assets only; some specific line of business IT assets are identified as out of scope.

Business areas in scope of this AMP include:

- Finance. This is inclusive of:
    - Finance;
    - Supply Chain;
    - Fleet;
    - Facilities;
    - Business Services.
- People/Health Safety & Environment;
- Digital Transformation & Strategy;
- Operations;
- Customer Services;
- Governance;
- Stakeholder/Regulation; and
- Strategic Growth/Major Projects.

3.2 Out of Scope

The following categories of Digital Assets are out of the scope of this document and are addressed in separate asset management plans:

- Infrastructure, including: Security, Servers, Desktops (Standard Operating Environment and supporting technologies) and Networking, managed by the Digital group;
- Network Operation and Control System (NOCS) software assets, managed by the Operational Systems team;
- Communication software assets, managed by the Telecommunication Network Operation and Control System (TNOCS) team;
- Protection and control software and networks assets, managed by the Protection and Control team;
- Asset Management Information System (AMIS) Improvements managed by the Digital Solutions team, with the exception of the ERP system.

4 Management Strategy and Objectives

This asset management plan has been developed to align with both TasNetworks' Asset Management Policy, Strategic Asset Management Plan and Strategic Objectives.

Our Digital Technology Strategy is to modernise, maintain and improve the Digital Technology environment through the periodic updating and refreshing of applications, infrastructure, and vendors to achieve the lowest cost to operationally manage and support Digital Technology and deliver corporate and customer expectations.

TasNetworks recognises that the technology domains of Information Technology, Operational Technology, Telecommunications and Cybersecurity make up the key elements to providing TasNetworks with a modern, efficient technology environment.

We will achieve this by:

- Operating within the Board approved TasNetworks IT Governance Framework;
- Building the roadmap for the future TasNetworks Digital Technology Enterprise Architecture, inclusive of investment, prioritisation and phasing;
- Delivering solutions based on the lowest Total Cost of Ownership (TCO), inclusive of on-premises and cloud hosting and consideration of re-use, buy and build options;
- Actively pursuing strategic outsourcing opportunities by seeking partners, cloud and external agencies to deliver low value commodity services;
- Positioning TasNetworks for changes in delivery models for Digital Technology by vendors;
- Protecting TasNetworks' Digital Technology assets with a risk-based security model to reduce risk to as low as reasonably practicable; and
- Positioning TasNetworks Digital Technology as an enabler of future business agility and increased customer value by transforming the way we operate.

5 Operating Principles

Principles are general rules and guidelines, intended to be enduring and seldom amended, that inform and support the way in which an organisation sets about fulfilling its mission.

Principles are defined to govern a choice between valid alternatives and are relevant to the TasNetworks environment.

The discussion of principles has been broken into several themes including:

- **Enterprise principles;**
- **Business principles;**
- **Data principles;**
- **Application principles;**
- **Technology principles.**

5.1 Enterprise Principles

Table 2 – Enterprise Principles

Name	**Principle 1: Change must be managed**
Statement	All changes to architectural applications and technology across the business require formal architectural governance prior to establishing a solution.
Rationale	This principle will give each change proposal due consideration through a formal governance framework. A number of governance gateways are defined during the full life cycle of the change as defined in the endorsed project methodology. An architectural assessment is to be performed to ensure there is full consideration of the impact the solution will have on existing people, process, systems and technology. All legislation, regulation, license and corporate compliance obligations will be satisfied.
Implications	<u>Project clarity</u> • This principle requires that the business problem / issue / opportunity / impact is fully understood. • Gives a clear focus for what is to be changed so that scope and costs can be controlled. • Impact assessments can determine any issues / risks to reduce scope creep and unexpected outcomes. <u>Delivery into production</u> TasNetworks' endorsed project methodology is used to deliver changes into the production IT environment. <u>Solution architecture</u> TasNetworks' Enterprise Architecture framework is used to provide guidance for developing effective solutions within TasNetworks.
How to apply	All projects must be delivered using the endorsed project methodology supported by the Enterprise Architecture framework.

Name	**Principle 2: Reduce Unnecessary Diversity and Complexity**
Statement	Current systems and new solution proposals will seek to reduce diversity of technology and architecture whilst simplifying integration between applications.

Rationale	TasNetworks' total operational environment of business systems, integration and infrastructure is excessively complex. This increases operational expense burden and hinders flexibility and integration. Limiting the number of supported components will simplify maintainability and reduce costs.
Implications	<u>Standards</u> Standards for technology and architecture must be created as part of the TasNetworks' Enterprise Architecture capability. <u>Reuse</u> • License costs are reduced through economies of scale and re-use of existing enterprise licenses. • Fewer technology options introduced reduces the support skills required and has less work load for support staff to manage. • Any application that is replaced must have a plan to be decommissioned. <u>Rationalise</u> Optimise the number of systems or assets.
How to apply	All projects must follow the endorsed project methodology and consider the solution architecture of proposed solutions through the Architecture design process.

Name	**Principle 3: Optimise for Organisational Benefit**
Statement	TasNetworks' Digital strategy will first strive to leverage common solutions that address multiple needs and that provide enterprise wide benefits over silo solutions. Note: This principle does not imply that individualised solutions are not acceptable. Rather, it is emphasising the benefit of actively seeking to develop standardised solutions to business needs.
Rationale	• Within the Business, there will always be conflicting and competing projects and initiatives for the limited resources available. Keeping an enterprise wide perspective on this matter and on the allocation of limited resources is the most fair and equitable mechanism for resolving such conflicts. • Managing from the enterprise wide perspective (that is, across all groups) provides the best opportunity to identify duplications of effort, as well as to rationalise and reuse solutions. • The current autonomous division management within TasNetworks has led to duplications of effort and technology investment. • It is more cost-effective to have specialised skills (for example, business system administration, business analysts and project management analysts/programmers) within a central pool that is shared across the enterprise, rather than for the individual groups to carry the costs of such resources within their budgets. • The Business requires services that foster operational collaboration, cross-organisation information views, and highly adaptive, flexible enterprise wide solutions. • Adopting a holistic view within TasNetworks will maximise the potential synergies across organisational boundaries and increase the reuse potential of solutions developed.
Implications	• TasNetworks should review and assess its resources to determine how these resources are structured, in order to optimise their productivity and availability to all groups within TasNetworks. • TasNetworks should invest in a governance structure and compliance processes to enhance its investment evaluation, approval and resource allocation processes. • TasNetworks' governance processes must ensure that tailored solutions that address unique requirements are strictly managed to avoid incremental divergence from the EA over time. • Ensure resource optimisation through shared platforms, implement shared application and database instances where possible. Remove single instance environments through active lifecycle management. Shared platforms are the default. New environments will utilise

	shared resources, or where capacity is restrained, shared resources will be created. Virtual environments are the default unless technically inappropriate or un-supported. • Infrastructure is a shared resource that aligns standards and technologies. Centralised storage, utilisation of server and network standards across the enterprise to reduce complexity and varied skill sets, are critical to reducing IT costs. Ensure no standalone systems exist in the environment unless restrained by technical design.
How to apply	N/A

Name	**Principle 4: Enterprise IT Assets Are Managed Through the Entire Life Cycle**
Statement	TasNetworks will recognise that assets (including technology assets) have a life cycle and manage the enterprise assets accordingly. It will also ensure that the total cost of acquisitions is defined over the entire life cycle of the asset and included in the business case supporting the acquisition. A simple version of the asset life cycle is as follows: • Emergence; • Mainstream or Core; • Replacement; • Containment; • Retirement.
Rationale	• Assets are like any element of an organisation requiring investment and management, and they include business processes, enterprise solutions, IT infrastructure and buildings. • Asset operation and maintenance costs often represent a significant percentage of the total cost of ownership over the total life cycle. • Assets are expensive and should be properly managed throughout the life cycle to ensure that the maximum return on the investment is achieved. • Assets are expensive, and understanding their life cycle expectancy will help TasNetworks to prepare, schedule, budget and plan for their eventual replacement. • New assets must be of sufficient maturity and their risks clearly understood before they can be adopted. • Every major IT investment is a corporate asset and should be managed accordingly.
Implications	• TasNetworks should review its procurement policy, including its business case template, to ensure that it adequately reflects the organisation's adopted asset life cycle and that the total cost of ownership is considered in all acquisitions. • TasNetworks should centralise its IT asset procurement processes. • Products and technologies used by TasNetworks will be modern solutions already proven by significant adoption in the industry, thereby minimising technological and support risks. • If reasons exist to adopt new IT assets, then this is to be done in a controlled environment and in such a fashion that a decision not to adopt the asset produces no ill effects for the business.
How to apply	N/A

Name	**Principle 5: Risk Management**
Statement	From time to time, risks must be taken. Risk decisions must consider business need and will be taken based on appropriate architectural governance and stakeholder consultation.
Rationale	All IT investments must have risk assessments and mitigating strategies included to ensure the risk profile is acceptable.

Implications	Risk Assessments • Change proposals involve benefits, costs and risks assessments. All changes need the risk factors identified so an informed decision can be taken. • There are risks associated with implementing change and there are risks associated with NOT implementing change. • All risks are manageable with suitable mitigation strategies, trade-offs and finally risk acceptance. • The determination of acceptable residual risk is documented in TasNetworks' Risk Management policy. Emerging Technologies Risk implications of emerging technologies must be considered and understood.
How to apply	All projects must follow the endorsed project methodology including the risk management process.

Name	**Principle 6: Risk-Based Security**
Statement	IT assets will be protected with appropriate security based on risk
Rationale	There must be a business reason to access, modify, create and delete business data. All staff will have the access to the systems, information and IT equipment necessary to perform their role. IT systems will have risk assessments to ensure appropriate levels of access. IT systems will ensure the implementation of an audit trail of changes to ensure appropriate control. External organisations that receive and manage TasNetworks' data will have security risk requirements included in contracts. Technology introduced without security risk assessment can have catastrophic effect on the entire IT infrastructure.
Implications	Security assessments • Risk based security assessments give consideration to the impact and probability of the loss, so that the cost to implement suitable mitigating strategies is warranted and represents value for money. • Security will use role-based access model. • Security is to be provided using different methods that should work together to provide the needed control of the business's processes and systems. Government Information Security Policy • TasNetworks and TasNetworks' systems are required to adhere to the Government Information Security Policy and other regulations and compliance obligations. • Financial and customer data must be encrypted before being sent to offshore locations. • Systems must comply with PCI DSS Reference Guide regulations Roadmaps are developed to include upgrade plans and refresh cycles – each system will be maintained to ensure it is supportable and has a planned and managed lifecycle. Legacy systems will be replaced by compliant, up to date environments that are standardised and supportable Aligned to the Digital strategy, security will be managed by risk. Each system will provide the minimum levels of access to ensure the business can use the system without compromising function. Access to systems will only be granted where it is needed and doesn't expose the business to risk. All systems to be capable of providing inputs to centralised auditing and logging environments, and comply with complex password lifecycle management. New systems will be implemented with security an integral part of the design.
How to apply	All projects must consider the security and identify appropriate measures to minimise risk in the solution definition.

Name	**Principle 7: Ensure Effective Corporate Compliance**
Statement	TasNetworks will acknowledge its corporate obligations and invest in change programs that are compliant with the corporate requirements imposed upon it
Rationale	• Corporate breaches have significant political, social, legal and cost implications. • TasNetworks must be able to demonstrate how it is socially and economically acquiescent to the process of government and must lead by example in its adherence to legislative requirements. • Being a good corporate citizen can enhance credibility.
Implications	TasNetworks must be cognizant of all its corporate requirements, including: • Occupational health and safety; • Equal employment opportunities; • Privacy Act; • Right to Information; • Religious and cultural expectations; • Public Interest Disclosures TasNetworks must review its current performance against corporate requirements, identify any breaches and address them immediately.
How to apply	All projects must follow the endorsed project methodology including the assessment of any obligations in their scope areas.

Name	**Principle 8: SAP is a Critical Business Platform**
Statement	Core to the TasNetworks Technology Strategy is the ERP which is the central enterprise platform.
Rationale	The SAP integrated ERP is a fundamental foundation supporting the TasNetworks driver to create "One Business" with global process standards and shared global data. The ERP platform is the core of the technology enterprise architecture.
Implications	Failure to fully leverage the ERP platform will likely result in sub-optimal returns on the significant investment. Additionally non-alignment increases the risks of perpetuating technology, process and resource duplication, and higher single point of failure levels.
How to apply	All Digital business systems and workflows will either adopt, or integrate with, the ERP solution. Any exception to this principle will be approved by the Executive Team.

Name	**Principle 9: IT, OT and Telco Convergence is critical to the Towards 2030 roadmap**
Statement	Globally the convergence of IT, OT and Telco Technologies is becoming not just a nice to have, but a must have in the corporate strategy of Utility companies.
Rationale	TasNetworks recognises that the technology domains of Information Technology, Operational Technology, Telecommunications and Cybersecurity make up the key elements to providing TasNetworks with a modern, efficient technology environment as outlined in our Future Distribution System Roadmap, Enterprise Asset Management Roadmap and TasNetworks Towards 2030 strategy.
Implications	The 2024-2029 Combined Proposal will need to take into account the desired level of capability in the 2030 strategy roadmap and ensure that the development of capabilities that support technology convergence is catered for.
How to apply	Continual review and alignment of Technology led projects to the 2030 strategy roadmap and maturity development monitored.

5.2 Business Principles

Table 3 – Business Principles

Name	**Principle 1: Primacy of Principles**
Statement	These principles of information management apply to all organisations within the enterprise.
Rationale	The only way we can provide a consistent and measurable level of quality information to decision-makers is if all organisations abide by the principles.
Implications	Without this principle, exclusions, favouritism, and inconsistency would rapidly undermine the management of information. Information management initiatives will not begin until they are examined for compliance with the principles. A conflict with a principle will be resolved by changing the framework of the initiative.
How to apply	N/A

Name	**Principle 2: Business Alignment**
Statement	IT exists to serve the business. IT proposals and decisions must demonstrate support of the Business Strategy, maximising benefit to the enterprise or the Tasmanian Electricity Industry as a whole. Proposals should align with the Digital Strategic Plan, Technology Roadmaps and Enterprise Architecture standards and policies.
Rationale	All business as usual IT proposals and decisions must identify measurable return on investment (ROI) over the full life cycle of the investment. (Government or Market reform initiatives will not be required to prove a positive ROI.) IT decisions must consider the long term strategic organisational perspective rather than short term project-specific or local business unit objectives in order to demonstrate a greater long term value.
Implications	Business Outcomes - The business must provide ratified statements of desired business outcomes, aligned to the business strategy. Whole organisational view - IT decisions taken on the basis of short term or local considerations can result in the duplication of technologies and therefore be detrimental to the organisation as a whole and to business transformation. Changes to the Strategy - Material external changes may require re-assessment of the Digital Strategic Plan.
How to apply	Any project must be aligned to the business and the Digital Strategy unless approval is provided by Digital leadership.

5.3 Data Principles

Table 4 – Data Principles

Name	**Principle 1: Data is an Asset**
Statement	Data is an asset. It has value to the end business and must be managed accordingly. Data is the foundation of our decision-making, so we must also carefully manage data to ensure that we know where it is, can rely upon its accuracy and can obtain it when and where we need it. Accurate, timely data is critical to accurate, timely decisions.
Rationale	Business data is a critical asset that can be used throughout the organisation, poor quality can lead to exacerbated issues across business units and processes. The data needs correct interpretation, so it needs to have clear definition and meaningful relationships with other data. Data must have credibility, so it needs to be of high quality. This will require the data to be accurate, up to date with negligible duplicate records. Data is to be duplicated only where necessary. Redundant or duplicated data must be planned and controlled; otherwise the data quality will erode over time resulting in poor data quality. There needs to be reduction in the number of existing duplicate data sources of similar data. Provision needs to be made contractually for outsourced application data to be accessible and correctable.
Implications	<u>Authoritative data source</u> • Data must have a primary authoritative source, this is to be well defined and understood. This may not be the raw source, but can be a consolidated data source. • Two or more applications cannot control the same data simultaneously. One of the applications has to be the master. Subtle errors / data anomalies will reduce data quality which results costly analysis and correction. <u>Duplication of data</u> • The cost of managing duplicate data is high due to the need to guarantee data integrity. Data synchronisation and transfer infrastructure is also quite expensive. • Standalone applications have a major duplication of data. All applications sharing data must be integrated with master data sources.
How to apply	All projects must consider the data architecture of proposed solutions through the Architecture design process. Where data attributes are not contained within the Logical Business Data Model, these need to be added and defined by the Data Architect to ensure consistent use ongoing.

5.4 Application Principles

Table 5 – Application Principles

Name	**Principle 1: Use, Buy, Build**
Statement	TasNetworks' Digital strategy is to use existing investments in systems and infrastructure where possible. If an existing system is not available or appropriate, then a software package with an acceptable level of support designed to be configured and extended by the customer (i.e. not requiring modification to core system code) is second preference. Software development will be approved only where the first two options are not possible or are inappropriate for the business requirements.
Rationale	TasNetworks has a strong preference to re-use existing systems to reduce unnecessary proliferation of technologies, solutions, architectures. Next is a strong preference to use technologies that are compatible with existing technologies, existing integration standards or support systems. This reduces operational support costs and facilitates integration of data and process.
Implications	Bespoke Development • Development will be considered only where re-use is not possible and acquisition of suitable, configurable, vendor-supported software packages either does not meet business requirements or timelines. • When timeframes or costs are prohibitive to business initiatives, we will deliver tactical solutions using the Microsoft .Net development environment using a methodology that ensures the system and business can be supported effectively.
How to apply	All projects must follow the endorsed project methodology and consider the solution architecture of proposed solutions through the Architecture design process.

Name	**Principle 2: Manage Vendor Lock-In**
Statement	Vendor lock-in happens in many ways as organisations balance solution costs against architectural flexibility. Understanding and managing lock-in are key to optimising TasNetworks' enterprise architecture for current and future needs.
Rationale	It's important to evaluate the potential degree of lock-in associated with any offering. Customer Experience The promoted value proposition of overall customer experience is that the vendor provides the Digital services so that customers can focus on their business. Business The promoted value proposition of adopting a vendor's business strategy is that the vendor has better ways to support the customer's business than the customer has. Digital Strategy The promoted value proposition of using a vendor-defined Digital strategy is that the vendor is considering architecture, and the vendor's services and technology are designed to work together. Tactical The promoted value to Digital leaders of using vendor-specific technologies and interfaces at a tactical level is increased interoperability and reuse. The business should consider the specific products, services, architecture, configuration, and licensing terms and conditions that the vendor is offering.

Implications	• Understand the potential benefits of aligning with a specific vendor's strategy, technology and services:
	  o Greater and higher degrees of functionality (for example, performance, integration and innovative features);
	  o High-volume discounts;
	  o More tightly integrated end-to-end solutions;
	  o Reduced costs of integration;
	  o Range of products available from associated vendors providing leverage;
	• Understand the potential costs of aligning with a specific vendor's strategy, technology and services:
	  o Reduced ability to integrate other systems (for example, applications, middleware and tools);
	  o Reduced ability to negotiate for specific discounts because of the limited ability to introduce competitive bids;
	  o Increased need for specialised technical skills (for example, system managers, programmers and relationship managers);
	  o Required upgrades based on product dependencies, not direct user value
	  o Limited choice of associated products;
	• Understand the risk/reward relationship between architectural freedom and business volatility and differentiation;
	• Do not try to define a corporate mandate or policy with respect to architectural vendor lock-in. Rather, weight the cost-benefit of lock-in relative to the organisation's diverse business requirements (a static non differentiated area of the business versus a dynamic and high-value area of the business) and the ability to invest in IT.

How to apply	All projects must follow the endorsed project methodology and consider the solution architecture of proposed solutions through the Architecture design process.

5.5 Technology Principles

Table 6 – Technology Principles

Name	**Principle 1: Infrastructure is Reliable**
Statement	Information and services are reliable, accurate, relevant and timely.
Rationale	Effective and efficient business and IT systems that provide consistent outcomes will enable the organisation to deliver value to our customers.
Implications	Redundancy and availability is core to design and build. Each system will ensure relevant levels of redundancy for the criticality of the system. Each system will be recoverable without loss of transactions or data. Business critical systems will use the standard TasNetworks' disaster recovery processes that utilise the data centre capabilities. Core infrastructure will have a planned and managed lifecycle that ensures technology stays current and capacity aligns to business requirements.

Name	**Principle 2: Infrastructure that is Affordable and Sustainable**
Statement	Provide fit for purpose, cost-effective infrastructure solutions that return a business benefit.
Rationale	In order to deliver on our strategy to deliver real value to customers, the value and cost of infrastructure investments must be measurable in objective terms. Infrastructure that does not have either an understood return on investment, or align clearly to a strategic objective is unlikely to be sustainable.

Implications	Provide an environment that ensures scalable, low-unit-cost solutions; an environment that delivers what is required in an efficient manner. Infrastructure that is fit for purpose and is aligned to the type and size of the business needs and technology standards. Standardised, best-practice infrastructure with a proven support framework.

Name	**Principle 3: Infrastructure that has Consistent Interoperability**
Statement	Deploy systems that use widely accepted standards and integrate easily, creating an environment in which information can be readily exchanged and shared.
Rationale	A high degree of natural integration between systems can reduce complexity, increase skills availability and reduce support costs.
Implications	Infrastructure should be designed to be interoperable and consistent. Interoperable capabilities will be available across all areas including business processes, information, applications and technical assets. Seek to reduce integration complexity.

Name	**Principle 4: Infrastructure is Managed and Automated**
Statement	All systems and environments are monitored and managed with standard, integrated and centralised platforms, Processes are automated to reduce support costs and remove manual processes.
Rationale	Effective monitoring will assist to improve the reliability of services, and automating that monitoring where possible will help to keep support costs down.
Implications	Appropriate toolsets will be provisioned to ensure that total visibility and control of the infrastructure assets is possible. Assets are managed and audits routinely conducted.

6 Asset Management

6.1 TOGAF at TasNetworks

TasNetworks uses the approach provided by 'The Open Group Architecture Framework' (TOGAF) to provide a structure to plan and manage its Corporate IT assets.

TOGAF is a framework including a detailed architectural development method and a set of supporting tools for developing an enterprise architecture (for a high level description of TOGAF see link High level description of TOGAF).

TasNetworks has created architectural processes, repositories and artefacts for its in-house tailored implementation of TOGAF. The TasNetworks process is described in the section 6.5 Methodology to Create Program of Work for the 2024-2029 Combined Proposal.

Core to TOGAF is its Architecture Development Method (ADM) which is a detailed, step-by-step method on how to build, maintain and implement enterprise architecture. It consists of 8 different steps in a design cycle as shown in the following diagram.

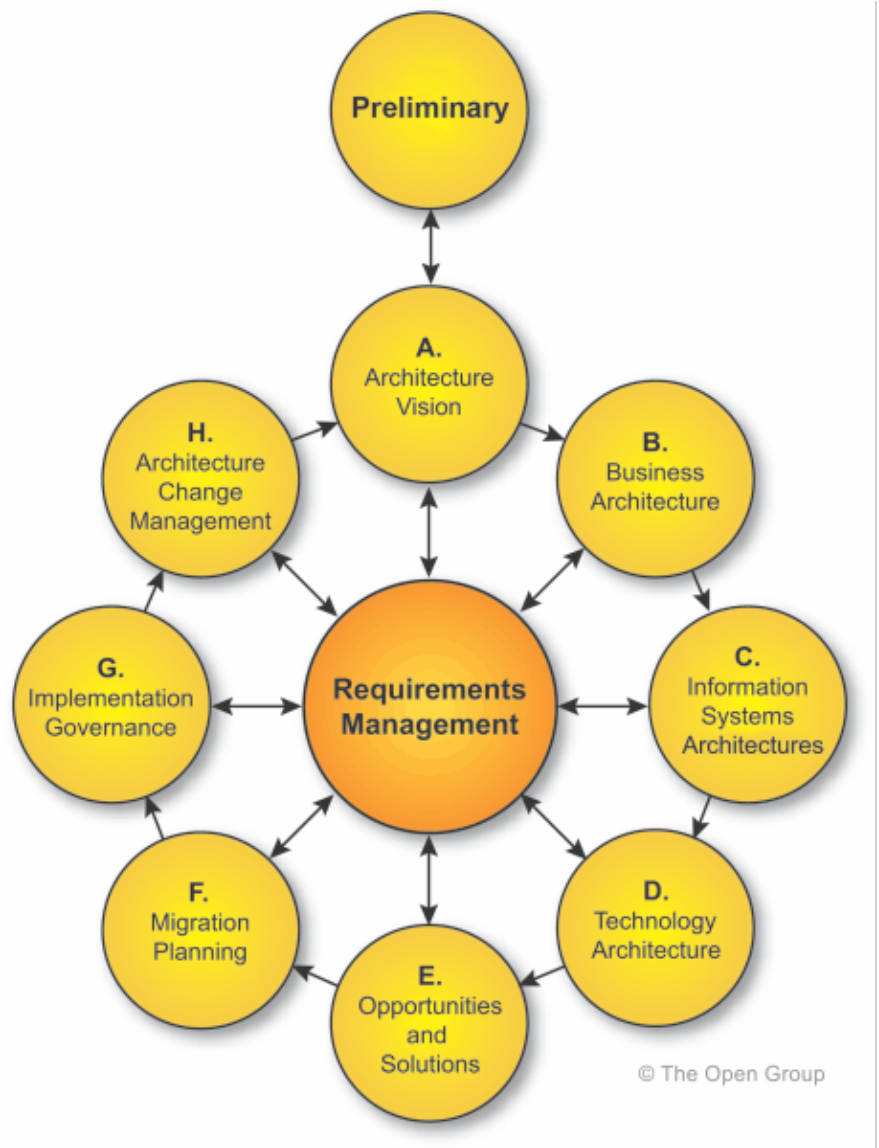


Figure 1 – Representation of TOGAF ADM

6.2 Application types

TasNetworks categorises its applications into six different types:

- Software (includes server software and desktop clients);
- Web applications;
- Server software;
- System interfaces;
- SharePoint applications;
- Software-as-a-service.

6.2.1 Software

Software encompasses desktop clients and server software.

Desktop clients are all those software packages that must be installed locally on a business user's computer. Software installed on a user's computer that communicates with server components, including databases, are still considered desktop clients. However, the server components may be separately registered as 'server software' depending on their nature.

The critical asset management considerations for desktop clients are:

- Packaging and deployment of the software and any updates to user computers;
- Compatibility with other desktop software and driver requirements;
- Communication requirements, particularly with server components.

Server software packages are any software packages designed to be installed on a server operating system rather than on a user's computer, but for the purposes of this asset management plan exclude web applications. Server software can be accessed directly by users, accessed indirectly by users of web applications and desktop clients that connect to the software, or may not be accessed by users at all.

Critical asset management considerations of server software are:

- OS version, software and database dependencies;
- Compatibility with other server systems, including compatibility of pre-requisite components;
- Integration capabilities (API etc.);
- Capacity management of server bandwidth, storage, memory and CPU.

6.2.2 Web application

TasNetworks manages a wide range of web applications. Web application are built using internet technologies, installed on a server and accessed by users using a web browser client. In most cases, it is the preference of the corporate Digital group to procure and implement solutions that are web applications. This is due to the high-level of internal skills available to support and develop systems built on web technologies, the simplified deployment model and the ability to make systems mobile device-friendly without excessive additional costs.

Critical asset management considerations for web applications are:

- Whether the business requirements can be met by web technology. Some solutions still need to be implemented as a fully featured desktop client;

- Capacity management of server bandwidth, storage, memory and CPU;
- System security and protection, especially for any systems exposed outside the Corporate IT network.

6.2.3 System interface

System interfaces connect disparate software systems to provide functional integration. At TasNetworks they are predominantly built using web services, SAP Process Orchestration and Microsoft SQL Server Integration Services. Appropriate use of system interfaces enables TasNetworks to reuse components and functions, extend software features and reduce the cost of development, support and maintenance.

Critical asset management considerations of system interfaces are:

- Appropriate governance of system changes and utilisation;
- Strong change management to protect against the much greater level of complexity born of system interdependencies;
- System security and protection, especially for any interfaces exposed outside the Corporate IT network.

6.2.4 SharePoint application

Microsoft SharePoint is used by TasNetworks as a comprehensive application platform.

Critical asset management considerations for SharePoint applications are:

- Capacity management of server farm bandwidth, storage, memory and CPU;
- Software update requirements; SharePoint platform upgrades may be driven by considerations external to specific systems implemented on SharePoint, affecting the software lifecycle.

6.2.5 Software-as-a-Service

An ever-increasing number of vendor software solutions are being offered as Cloud / Software-as-a-Service. SaaS is provided via a secured internet site rather than installed locally on the TasNetworks Corporate IT network. This service model has the potential to save the business money under certain circumstances, but also introduces a range of new challenges to the management of Digital.

Critical asset management considerations for Software-as-a-Service are:

- Vendor reliability and Service Level Agreements;
- Physical location of data centres and jurisdictional or legal requirements;
- Privacy and security of data;
- Integration requirements with other systems;
- Transition planning: ability to safely or securely transition to a different solution in the future;
- Risk to operational processes, including staff or customer safety or electricity supply.

6.3 Monitoring

The corporate Digital group has adopted a strategy of implementing both proactive and reactive condition monitoring of IT assets, including physical assets, virtualised or physical infrastructure assets and software assets. Proactive monitoring practices actively check the condition of IT assets to identify developing

condition issues before they could result in an incident[1]. Reactive monitoring detects incidents once they have occurred so that normal service can be restored.

6.3.1 Proactive monitoring

The goal of proactive monitoring is to predict likely incidents with sufficient notice and information to enable Digital staff to take corrective action and avoid an incident.

TasNetworks implements two strategies for proactive monitoring:

1. Continuous system monitoring - Corporate IT has implemented condition monitoring for software assets to detect defects and issue early warning of developing issues. TasNetworks has an operational monitoring system that displays system and infrastructure statuses and alerts on dashboards in the IT area as well as email and SMS alerts to infrastructure personnel in real-time. This system tracks:

    - Server physical state (powered on or off);
    - Server responsiveness;
    - CPU utilisation;
    - Memory utilisation;
    - Disk space;
    - SQL server instance states;
    - IIS state and responsiveness;
    - Application service states;
    - Application log file activity.

    In addition to the operational monitoring system, the underlying virtualised infrastructure is monitored using VMware's active monitoring, and daily checklists are followed to confirm systems are operating within expected parameters.

2. Periodic application health checks – TasNetworks routinely conducts application health checks with business representatives. This process is represented in Figure 2 – Health assessment process. The process has 3 main steps which result in a business and technical health scores and an overall application health score.

    Step A - To evaluate the business health a set of key users are asked to score a set of standard questions which ultimately roll up to an average health score. Users were asked to rate the following questions on a scale of 1-5 where 5 represents optimum health:

        - What is the quality of the data in the system?
        - How accessible is the data in the system?
        - How well does this application meet the business requirements?
        - How well will this system meet future business needs?
        - How would you rate user satisfaction?
        - How efficient is the system at completing operations?

[1] Under ITIL, an incident is identified as any unplanned event that results in a loss or degradation of service.

- How responsive is the system to user actions?
- How available is the system (in reference to SLA requirements)?
- How reliable is the system?
- How many manual processes or 'workarounds' are used, and what is the FTE cost of these?
- How much revenue is at stake during a system outage?

Step B - In parallel to the business health evaluation, an assessment of the health of the supporting infrastructure is undertaken. Each of the following topics is considered and rolled up into an overall technical health score for each application:

- Recoverability;
- Hardware warranty;
- Operating System currency;
- RDBMS / platform currency;
- Storage conformance;
- Backup strategic alignment;
- Support contract;
- Hardware currency;
- Software/firmware currency;
- Redundancy;
- Monitored;
- Strategic Alignment.

Step C - Each key application is then given an overall application health based on:

- Business health;
- Technical health;
- Criticality;
- Vendor health/roadmap;
- Regulatory obligations;
- Emerging and potential technologies.

These activities result in an architectural blueprint of the corporate Digital group's business applications in their current and future predicted state where each application is diagrammatically represented by an elongated oval with colour coding to represent the overall application health.

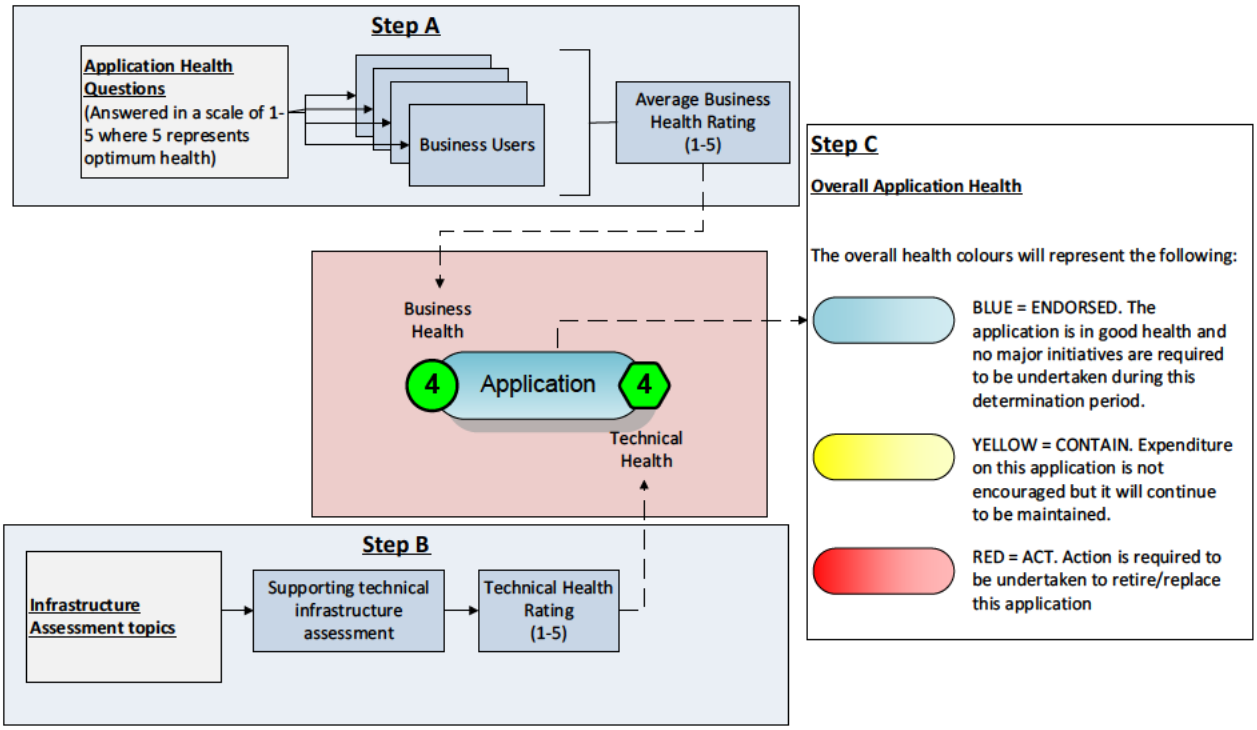


Figure 2 – Health assessment process

6.3.2 Reactive monitoring

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 in the shortest practical timeframe, and also provide that information to an appropriate person/system in a form that initiates the TasNetworks incident management procedure.

Corporate Digital has adopted multiple layers of reactive condition monitoring, which in addition to providing proactive alerts, also issues incident alerts. Separate to this, most software assets are configured with error logging and alerting, in most cases sending alerts to the Service Desk when an incident occurs.

Finally, Corporate Digital operates a manned Service Desk and a self-service portal for staff to report incidents as they occur.

6.4 Defect management

The corporate Digital group has implemented ITIL compliant incident and problem management processes that are applied to detect defects (incidents) in software assets.

6.5 Methodology to Create Program of Work for the 2024-2029 Combined Proposal

TasNetworks has employed the TOGAF Architecture Development Method (ADM) as the methodology for guiding and determining IT Systems capital expenditure decisions.

TasNetworks' methodology to create the Program of Work during the 2024-2029 regulatory control period follows the TOGAF ADM top down approach of identifying opportunities by starting with the corporate vision. The method is also supplemented/cross matched with bottom up approaches such as application health checks and maintenance regimes to ensure all 'change drivers' or issues are identified.

The methodology to create the program of work for the 2024-2029 regulatory control period is represented in the following diagram.

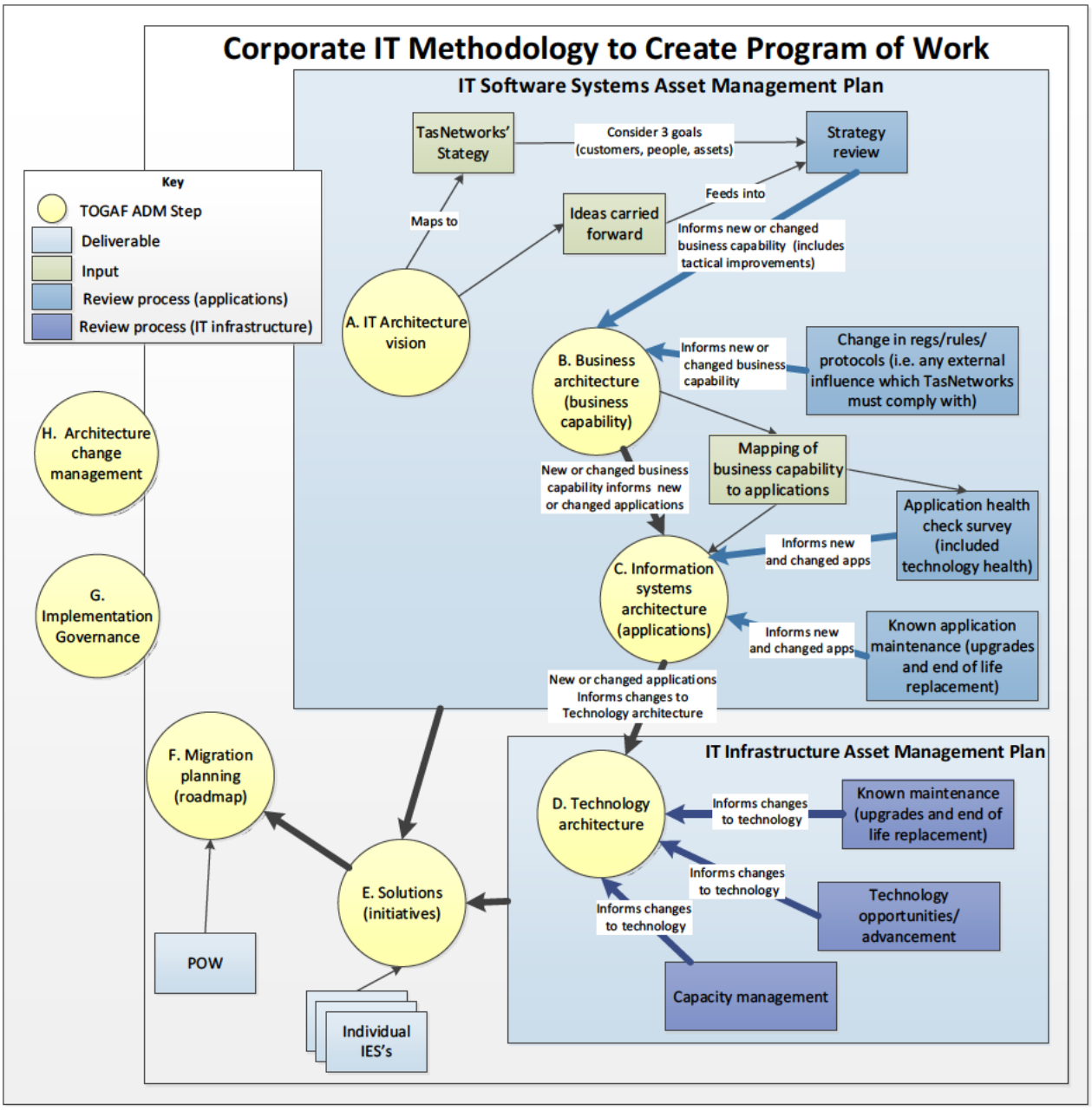


Figure 3 – R24 Corporate IT methodology to create program of work

The individual steps comprising the TasNetworks methodology to create the program, an adaption of the TOGAF ADM, are further elaborated below:

- **'A. IT. Architecture Vision'** – This is a top-down approach to identify new/changed business capability requirements. The business strategy review primary objective was to engage with the business and senior management in aligning Digital strategic planning with current and future business needs. It was an opportunity to ensure the business had an understanding and appreciation of the potential value of IT to the business and to then consider the current IT capabilities and asset performance, with a view to what will be required in the future. Using a list of ideas that had been compiled since the last regulatory documentation process, corporate Digital conducted workshops with various parts of the business to confirm the ideas were still valid and to also explore other new ideas. The list of ideas was evolved and rationalised.

The top down approach also included an analysis of changing Distribution Network Service Provider (DNSP) and Transmission Networks Service Provider (TNSP) regulatory related rules that TasNetworks operates within and is obligated to conform with[2].

- **'B. Business architecture'** - The outcome of the top down approach was a number of identified new or changed business functions that would need to be supported by corporate Digital applications.
- **'C. Information systems'** - TasNetworks also employed bottom up approaches to supplement the top down approach.

  Business and technical health of applications classed as critical, major and important were reviewed. The changed business architecture identified from the top down approach was distilled with known maintenance regimes[3] and the health check to identify a number of applications that need to be considered for change. It also identified gaps where new business capability had been identified without an obvious supporting application.
- **'D. Technology architecture'** - Changes to the application landscape is evaluated as part of the Information Systems review which is documented separately in the IT Infrastructure Asset Management Plan (see document titled 'Corporate IT - Infrastructure Asset Management Plan').
- **'E. Solutions'** - Using the IT operating principles, the new/changes to business capability and applications was used to identify a number of 'change drivers' or issues, which was rationalised into a list of potential initiatives.
- **'F. Migration Planning'** - The potential list of initiatives is evolved, prioritised[4] and costed[5] as a means of building the program for the 2024-2029 regulatory control period. Some initiatives have been identified as being necessary before the regulatory control period starts, and after the application of prudency, some are identified as being aspirational and for consideration in the next regulatory control period.

[2] TasNetworks utilises a number of bespoke (internally developed) and commercial off the shelf (COTS) systems to support mission and business critical Network and Customer Management business processes. These systems are required to operate and comply with the requirements of the following regulations and legislation:

- Australian Energy Market Operator (AEMO) and National Electricity Market (NEM) regulations;
- Distribution License - Issued by the Regulator (Otter) under the Electricity Supply Industry Act 1995
- National Energy Customer Framework (NECF);
- Commonwealth Taxation Law; and
- The National Electricity Law and the National Electricity Rules (NER) legal framework.

[3] Maintenance regimes of small to medium are formally captured in a 'business management systems' register. Maintenance for large applications are negotiated and scheduled far in advance after close liaison with vendors.

[4] Initiative prioritisation was based on classifying initiatives (in order of priority) as 'regulatory', 'must have', 'need to have', or 'nice to have'. Within each categorisation, the initiatives are ranked.

[5] Costs were estimated on combination of vendor costing, historic spend and internal estimates.

7 Initiatives (2022)

In the context of this Asset Management Plan, initiatives are prospective individual packages of work that ultimately form the 2024-2029 Program of Work and Roadmap. Although the intention is that these initiatives are undertaken during the timeframes proposed, a more detailed business case and evaluation process is still expected to be undertaken.

7.1 Drivers

The following is a brief discussion on the primary drivers for expenditure within the Non-Network Program of work.

7.1.1 AER Recurrent / Non-recurrent Classifications

The AER ICT Guidelines detailed a classification system that separated Recurrent and Non-Recurrent expenditure. In our experience this is not easily achieved:

- Projects to achieve new compliance obligations often involve a large component of technology uplift that we classify as 'Maintain existing services functionalities and capabilities'.
- Projects to achieve a new or expanded service can require similar regular upgrade activities

Therefore TasNetworks assesses the ratio of Recurrent / Non-recurrent costs involved with a project or program.

7.1.2 Distribution / Transmission Classifications

Many software assets are shared across Distribution and Transmission activities. For Revenue Reset submissions each Project or Program has an individually assessed ratio of Distribution / Transmission cost allocation.

7.1.3 Maintain existing services functionalities & capabilities

As previously described, a health assessment was conducted for the purposes of the Combined Proposal. As a result of the health assessment, the business, technical and overall health of the major business applications at TasNetworks was established. This enabled Corporate IT to build an architectural depiction of the current state of the business applications, as well as identify the following:

- Applications not supporting business needs;
- Current issues and defects with functionality and business processes;
- Manual workarounds in place due to software deficiencies;
- Performance and availability issues;
- Applications at risk of not being able to meet future needs;
- Opportunities for integration;
- Under-utilised/under-deployed applications.

The following initiatives are examples of being driven primarily through Asset End-of-life:

- Market Systems – MDMS Replacement/Major Upgrade ([redacted]);
    - Assessed as 100% Distribution

    - Despite the platform having upgrades applied during the last 5 years, it has been assessed as 100% Non-recurrent due to the likely platform replacement aspect of the initiative.
- Asset & Servicing Works Mgt. Tool Consolidation & Replacement ([redacted]);
    - Assessed as having a ratio of 75:25 Distribution:Transmission
    - This initiative affects a number of applications which may have had some upgrades during the last five years, however it has been assessed as 100% Non-Recurrent due to the major consolidation nature of the initiative.
- Design & Estimating Systems replacement.
    - Assessed as 100% Distribution
    - This initiative affects a number of applications which may have had some upgrades during the last five years, however it has been assessed as 100% Non-Recurrent due to the major consolidation nature of the initiative.

The following initiatives are examples of being driven primarily through Regular Maintenance:

- ERP – Upgrades & Enhancements Program;
    - Assessed as having a ratio of 75:25 Distribution:Transmission
    - Assessed as having a ratio of 66:33 Recurrent:Non-recurrent
      This initiative will involve regular upgrades to the product however will also involve activities that would be classed as Non-Recurrent such as:
      - Changes involved in updated Tax laws
      - Changes around strategic changes to the business
- MDMS – Upgrades & Rule Change Program
    - Assessed as 100% Distribution
    - Assessed as having a ratio of 70:30 Recurrent:Non-recurrent
      This initiative will involve regular upgrades to the product however will also involve activities that would be classed as Non-Recurrent such as regulatory driven changes to Market procedures & rules.
- Business Systems Maintenance
    - Assessed as having a ratio of 80:20 Distribution:Transmission
    - Assessed as having a ratio of 100% Recurrent
      This initiative will involve regular upgrades to 140 different applications
- Data and Analytics Program
    - Assessed as having a ratio of 75:25 Distribution:Transmission
    - Assessed as having a ratio of 100% Recurrent
      This initiative will involve regular upgrades to data & analytics applications

The current health of the key applications in the business is illustrated in the following diagram.

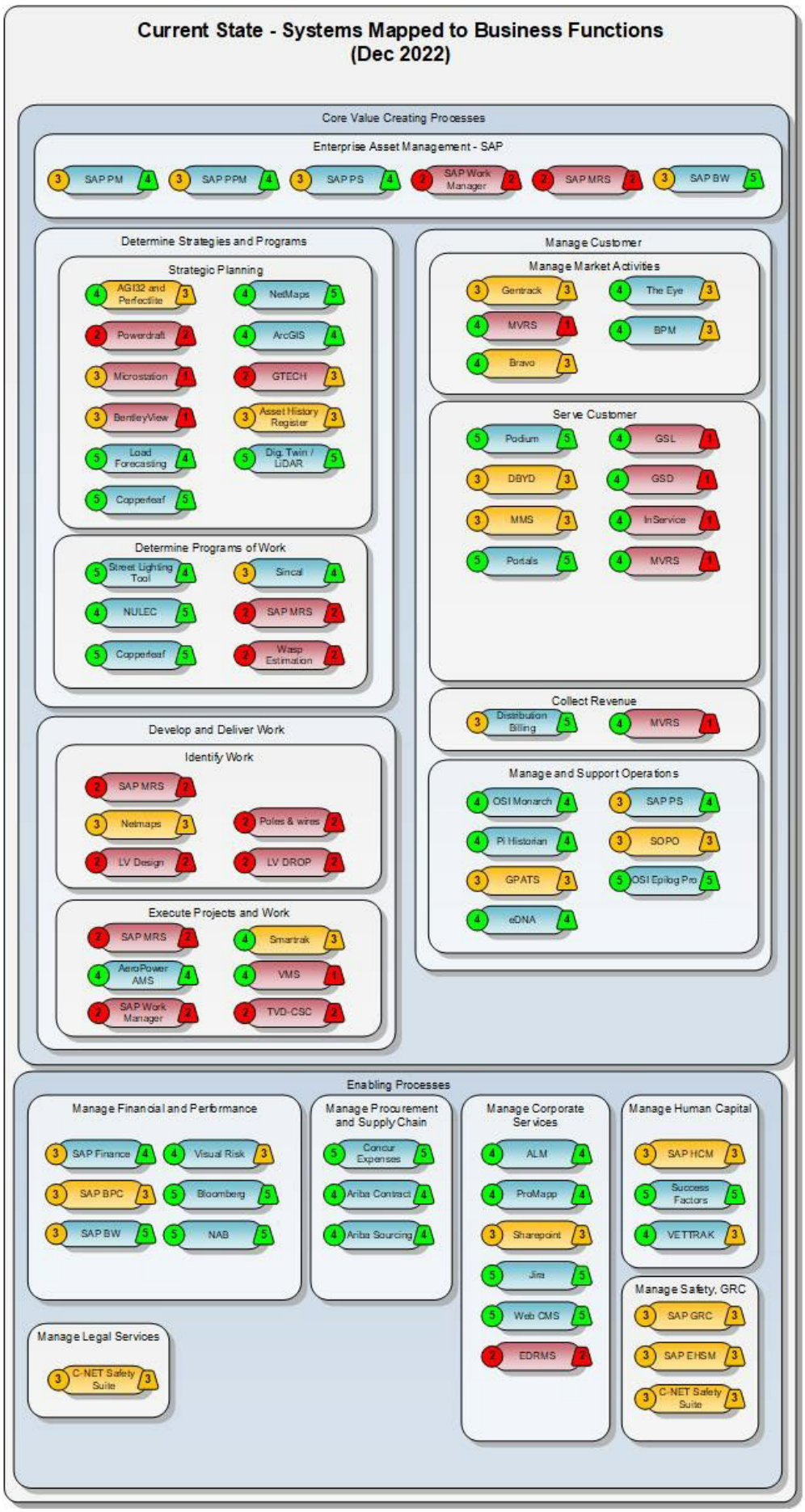


Figure 4 – Current core application health state as at November 2022

7.1.4 Comply with new/altered regulatory obligations / requirements

Projects to achieve new compliance obligations often involve a large component of technology uplift that we classify as 'Maintain existing services functionalities and capabilities'.

Therefore TasNetworks assesses the ratio of Recurrent / Non-recurrent costs involved with a project or program.

TasNetworks is required to maintain systems and procedures at a market-compliant level under the National Electricity Law (NEL) and is audited for this market compliance in at least Metering Provider (MPB) and Metering Data Provider (MDP) roles on a bi-annual basis to ensure compliance to market rules, procedures and service level requirements. Failure to maintain market compliance can result in the loss of accreditation to operate in these roles under the market.

During the next determination period, a number of regulatory and legislative changes are expected to occur that will require investment in our current market-facing and support systems to ensure ongoing compliance.

7.1.5 Acquisition of new or expanded services, functionality or capabilities

Projects to achieve a new or expanded service can require similar regular upgrade activities.

Therefore TasNetworks assesses the ratio of Recurrent / Non-recurrent costs involved with a project or program.

7.2 Major Initiatives by Functional Area

The following section outlines proposed expenditure described by the business functional area.

7.2.1 Business System Upgrades

TasNetworks operates a large number of smaller software applications to support the entire business. These will need to be upgraded during this regulatory period to ensure service reliability, maintain performance and manage corporate risks. In addition, evolving business environments and objectives often alter business requirements for software.

The software solutions covered by this program of work are integral to the successful operation of TasNetworks and include around 140 applications that can be roughly grouped into the following categories:

- Customer Systems (includes Public websites, customer complaint/enquiry & connection application portals, contractor portals, case management systems, dial-before-you-dig, payment systems)
- Collaboration and Document Mgt systems
- Outage Message Mgt, Outage Calculation & Reconciliation systems
- Engineering Applications
- Power Flow, Analysis, Monitoring & Modelling systems
- Design, Drafting & Drawing Mgt systems
- Training & Licence Mgt
- Finance, Banking & Risk systems.

TasNetworks is continuously exploring ways to increase its efficiency and improve effectiveness. These are often being achieved through the strategic implementation of software solutions to streamline and automate business processes, or even make some processes obsolete. As such, demand from the business for Information Technology (IT) application services remain consistently high and is not expected to decrease during the forthcoming regulatory period.

The consolidated initiative for of upgrades and/or replacement of various small applications is Business Systems Maintenance.

7.2.2 Data Warehouses, Business Intelligence and Analytics

TasNetworks is currently addressing the lack of a single enterprise data warehouse/reporting platform by building a data warehouse [redacted] and instituting a range of data management standards and processes.

This is making available data from multiple business domains. It is also providing self-service analysis (via SAP Analytics Cloud) and self-service data maintenance to reduce IT dependence.

However, significant further work is required, driven by the following trends:

- Rapidly increasing date volumes, complexity and varieties of formats
- Decentralisation of the analytics function into business areas
- Availability of analytics automation to remove complexity and make analysts more efficient
- Increasing integration complexity due to complexity of data and diversity of sources
- Opportunities to improve data quality using AI or machine learning
- The need for greater governance around the use of data and tools for analytics purposes

- The growing need for consumer data protection and privacy.

To address these trends the following initiatives will be undertaken:

- Completing the establishment of a data management framework and associated tools
- Upgrading data quality management tools
- Upgrading data integration tools
- Providing improved data analytics tools
- Supporting Democratisation of data analytics with tools and processes
- Establishing a unified data delivery and analytic platform.

Costs of this initiative are shared across Distribution and Transmission.

7.2.3 Customer Information Systems & Digital Engagement

TasNetworks has performed significant systems work during the current regulatory control period to enhance customer interaction via Web and Mobile channels and to assist in managing other interactions. Some minor enhancements are expected during the 2024-2029 regulatory control period, which have been included in the Business Systems Upgrades initiative.

This area will be reviewed again prior to the 2029-2034 Combined Proposal.

7.2.4 Enterprise Information Management

A project is underway to consolidate a number of Information Management systems within TasNetworks. This is expected to be completed in the latter part of the 2019-2024 regulatory control period. Consequently there is no funded initiative in this area planned for the 2024-2029 regulatory control period. It will be reviewed again prior to the 2029-2034 Combined Proposal submissions process.

7.2.5 Finance, HR, & payroll

Finance, HR and Payroll are principally supported by the ERP system. A number of modules in this suite are have reached or are nearing end of standard maintenance. This poses a risk from the point of view of potential system failure as well as the inability to apply updates to maintain legal compliance.

The proposed initiative is based on 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.

A major upgrade of the ERP to S/4HANA is recommended by the vendor. However, this will be a costly process and it is not essential until the end of 2030 when support will cease. Consequently it is proposed to delay that upgrade until the start of the 2029-2035 regulatory control period. Minor enhancements are also currently available to improve usability and increase efficiency. However, in order to demonstrate prudent expenditure it is proposed to defer these until the S/4 upgrade.

7.2.6 Asset and Works Systems

For the Distribution Business this topic includes:

a) Replacement of the Customer Connections Works Management Tool [redacted]

- This system is past end-of-life, it is now [redacted] years old and there is no upgrade path. Plans to replace this system in the 2019-2024 regulatory control period were deferred so it will now be included in the 2024-2029 regulatory control period.
- The work is vital to ensure customer facing connection services continue unaffected including;
  - [redacted] customer connections, [redacted] customer alterations / year
  - [redacted] customers moving in and out / year;

b) Replacement or upgrade of the Asset Based Works Management tools [redacted]. These systems are also at end-of-life and are not being supported by the vendor into the future.

In regard to the above two requirements, there is an opportunity to select and implement a single system to support works management for both Customer Connections and Asset Maintenance. An initiative is proposed to explore that option in addressing these systems.

c) Replacement of a range of design & estimating tools for Distribution Connections

[redacted]

The design team currently use a wide variety of un-integrated tools in the design process. This results in significant manual intervention in the process with resulting inefficiency. There are a range of other issues, including:

- Increased opportunity for errors
- Inability to enforce technical standards
- Lack of control and visibility of design documentation
- Lack of integration with ERP and GIS

Consequently an initiative is planned to replace the existing toolset with an integrated Design & Estimating solution with strong integration to a CAD foundation and easy use of standard design components.

There is no proposed expenditure in this area for Transmission in this period.

7.2.7 IT Infrastructure, Security & Support

This area involves various expenditures due to asset end-of-life or increased capacity requirements in the areas of End-user computing, IT Management and toolsets, IT Network Core Services, Collaboration Tools and Application Delivery Mechanisms.

The costs of these initiatives are shared across Distribution and Transmission.

7.2.8 Market Systems

Significant initiatives in this area include:

a) MDMS Replacement

The Market Data Management System replacement project will be started in the current period and will be completed in the R24 period as was specified in the R19 submission.

The system is instrumental in the processes of gathering and validating readings for the billing of Tasmanian basic metered customers.
This aging system holds significant market operability and compliance risks related to:

- Cash flow [redacted] of revenue processed through market systems)
- [redacted] million collected meter readings and [redacted] million generated reads for unmetered sites / year
- Compliance / operator licensing – a high risk that we can't achieve regulatory changes as technology ages.

b) MDMS Upgrades

The MDMS requires ongoing upgrades maintain currency of the software and to address any requirements from the biannual change program from AEMO. This change program alters procedure or data requirements for market participants. This is an ongoing compliance driven initiative which in R24 will dovetail into the MDMS replacement, with updates being applied to MDMS prior to go-live and to the replacement system thereafter.

8 Program of work

The presentation of the 10-year program of work has been broken into the program of work for the 2024-2029 regulatory control period (July 2024 to June 2029) and 2029-2034 regulatory control period (July 2029 to June 2034).

8.1 2024-2029 Program of Work

8.1.1 2024-2029 Roadmap

The following roadmap demonstrates the major initiatives proposed to be undertaken as part of the 2024-2029 Program of Work. The estimated commencement and duration of each initiative is shown, grouped by functional area.

Figure 5 – 2024-2029 Roadmap

8.1.2 Total Proposed Non-Network IT Program

The following information shows the profile across the R24 determination period.

Table 7 – Total Proposed Non-Network IT Program

Initiative	Year 1 2024-25	Year 2 2025-26	Year 3 2026-27	Year 4 2027-28	Year 5 2028-29	**Total**
Design & Estimation Completion	2,847,234	-	-	-	-	**2,847,234**
Market Systems - MDMS Replacement	9,208,253	11,067,000	-	-	-	**20,275,253**
ERP Upgrades & Enhancements Programme	2,675,823	2,675,823	2,675,823	2,675,823	2,675,823	**13,379,115**
Market Systems - MDMS Upgrades & Rule Changes Programme	3,158,823	3,158,823	3,158,823	3,158,823	3,158,823	**15,794,115**
Business Systems Maintenance - Minor Systems Programme	932,704	932,704	932,704	932,704	932,704	**4,663,520**
Works Management Tool platform upgrade	3,978,026	4,383,996	-	-	-	**8,362,022**
Data and Analytics Programme	1,736,082	1,286,654	1,286,654	1,286,654	1,286,654	**6,882,698**
Cyber Program	1,632,673	1,927,123	2,017,123	1,628,323	924,000	**8,129,242**
IT Infrastructure Core Services	1,715,328	5,600,448	1,663,989	2,798,712	2,646,384	**14,424,861**
Collaboration	1,117,729	1,133,703	1,154,691	1,142,217	1,002,231	**5,550,569**
End User Computing	646,409	554,345	2,427,353	516,305	600,915	**4,745,326**
IT Management and Supporting Tool-set	948,480	949,200	574,560	429,600	372,600	**3,274,440**
IT Security	604,800	735,000	252,000	218,400	572,040	**2,382,240**
Application Delivery	80,850	292,578	168,300	270,072	154,275	**966,075**
Totals	**31,283,213**	**34,697,396**	**16,312,020**	**15,057,632**	**14,326,449**	**111,676,710**

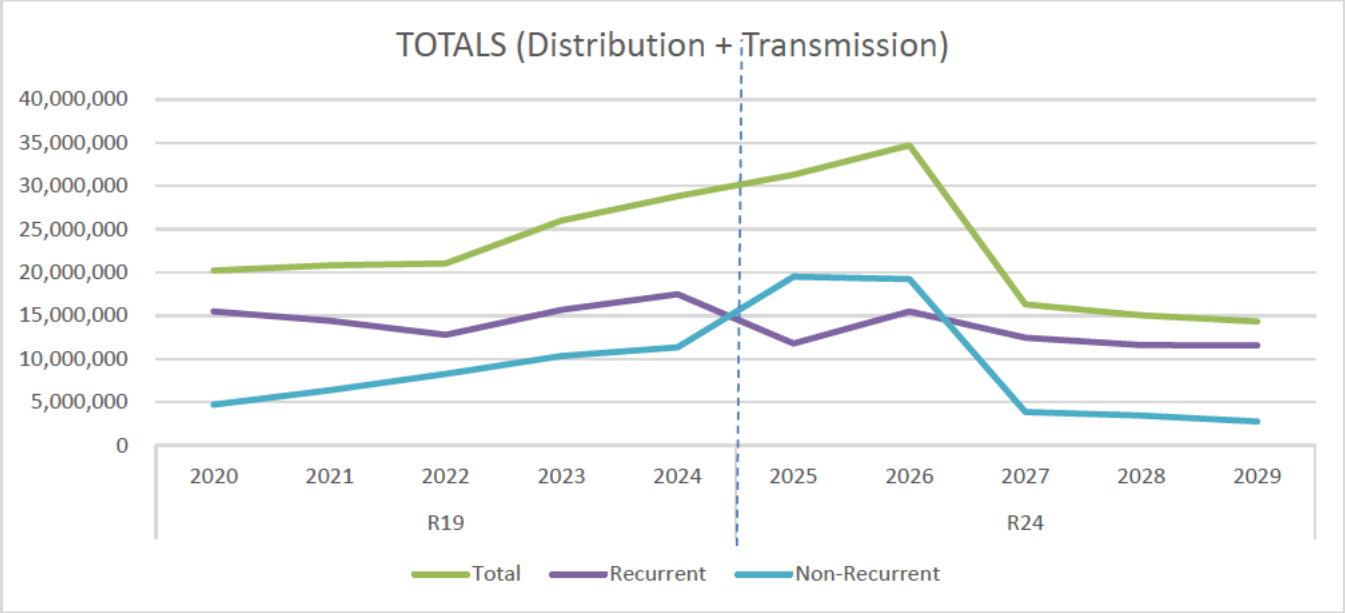
8.1.3 Recurrent & Non-Recurrent Profile across R19 & R24

The following information shows the profile across the 2019-2024 and 2024-2029 regulatory control periods.

Table 8 – Recurrent & Non-recurrent profile across the 2019-2024 and 2024-2029 regulatory control periods.

Period	R19					R24				
Year	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**2028**	**2029**
Total	**20,226,380**	**20,802,190**	**21,021,391**	**26,005,101**	**28,816,595**	**31,283,213**	**34,697,396**	**16,312,020**	**15,057,632**	**14,326,449**
Recurrent	15,498,839	14,409,865	12,768,175	15,675,282	17,477,798	11,777,440	15,479,689	12,455,309	11,589,721	11,562,861
Non-Recurrent	4,727,541	6,392,325	8,253,216	10,329,819	11,338,797	19,505,774	19,217,707	3,856,711	3,467,911	2,763,588

Figure 6 – Recurrent & Non-Recurrent Profile across the 2019-2024 and 2024-2029 regulatory control periods.



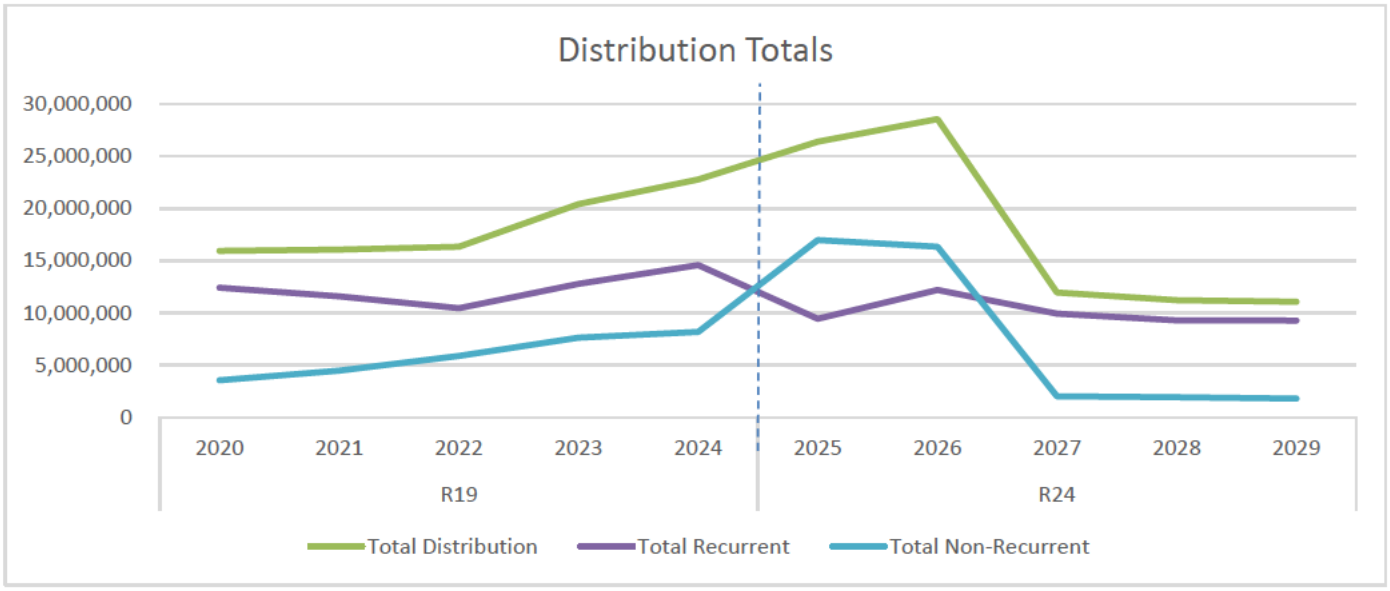
8.1.4 Distribution Recurrent & Non-Recurrent

The following information shows the Distribution profile across the 2019-2024 and 2024-2029 regulatory control periods.

Table 9 – Distribution Recurrent & Non-recurrent profile across the 2019-2024 and 2024-2029 regulatory control periods.

Period	2019-2024					2024-2029				
Year	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**2028**	**2029**
Total	**15,948,777**	**16,057,581**	**16,348,157**	**20,419,453**	**22,784,479**	**26,414,653**	**28,566,220**	**11,960,938**	**11,233,987**	**11,072,977**
Recurrent	12,408,534	11,575,885	10,454,208	12,784,056	14,583,758	9,432,509	12,209,196	9,940,911	9,291,720	9,271,575
Non-Recurrent	3,540,243	4,481,695	5,893,948	7,635,397	8,200,721	16,982,144	16,357,024	2,020,027	1,942,267	1,801,403

Figure 7 – Distribution Recurrent & Non-Recurrent Profile across the 2019-2024 and 2024-2029 regulatory control periods.



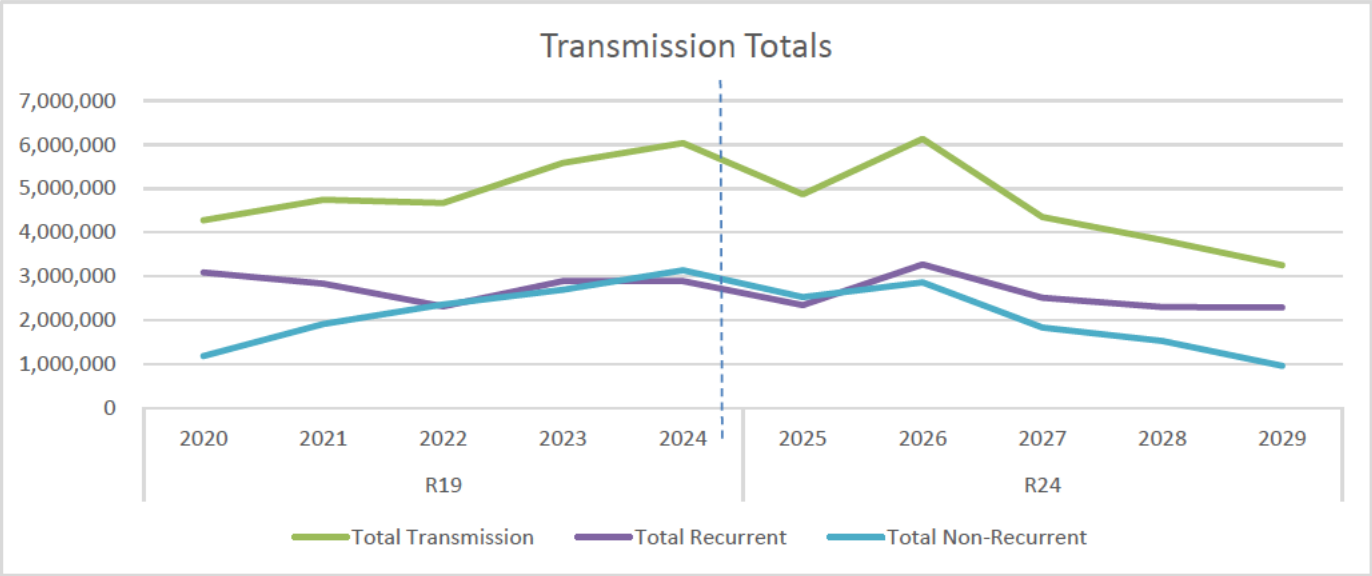
8.1.5 Transmission Recurrent & Non-Recurrent

The following information shows the Transmission profile across the 2019-2024 and 2024-2029 regulatory control periods.

Table 10 – Transmission Recurrent & Non-recurrent profile across the 2019-2024 and 2024-2029 regulatory control periods.

Period	2019-2024					2024-2029				
Year	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**2028**	**2029**
Total	**4,277,603**	**4,744,610**	**4,673,234**	**5,585,648**	**6,032,116**	**4,868,561**	**6,131,176**	**4,351,082**	**3,823,645**	**3,253,471**
Recurrent	3,090,304	2,833,980	2,313,966	2,891,226	2,894,040	2,344,931	3,270,493	2,514,398	2,298,001	2,291,286
Non-Recurrent	1,187,298	1,910,630	2,359,268	2,694,422	3,138,076	2,523,630	2,860,683	1,836,684	1,525,644	962,185

Figure 8 – Transmission Recurrent & Non-Recurrent Profile across the 2019-2024 and 2024-2029 regulatory control periods.



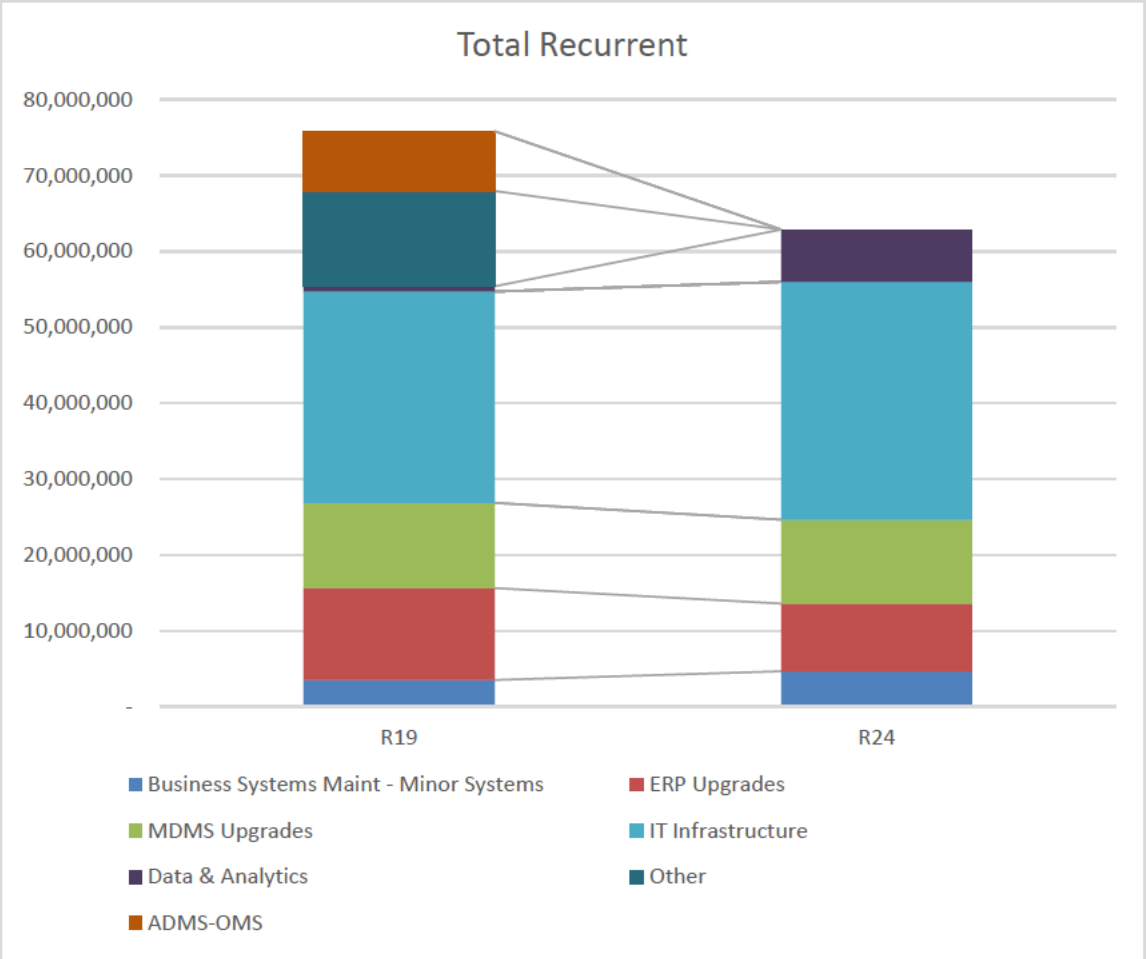
8.1.6 Total Recurrent Profile across R19 & R24

The following information shows the Recurrent expenditure profile across the 2019-2024 and 2024-2029 regulatory control periods.

Table 11 – Total Recurrent profile across the 2019-2024 and 2024-2029 regulatory control periods.

Category	2019-2024	2024-2029
Business Systems Maintenance	3,510,816	4,663,520
ERP Upgrades	12,113,360	8,919,410
MDMS Upgrades	11,233,952	11,055,881
IT Infrastructure	27,836,753	31,343,511
Data & Analytics	693,144	6,882,698
Other	12,557,550	-
ADMS-OMS	7,884,383	-
Totals	**75,829,958**	**62,865,020**

Figure 9 – Recurrent Totals across the 2019-2024 and 2024-2029 regulatory control periods.



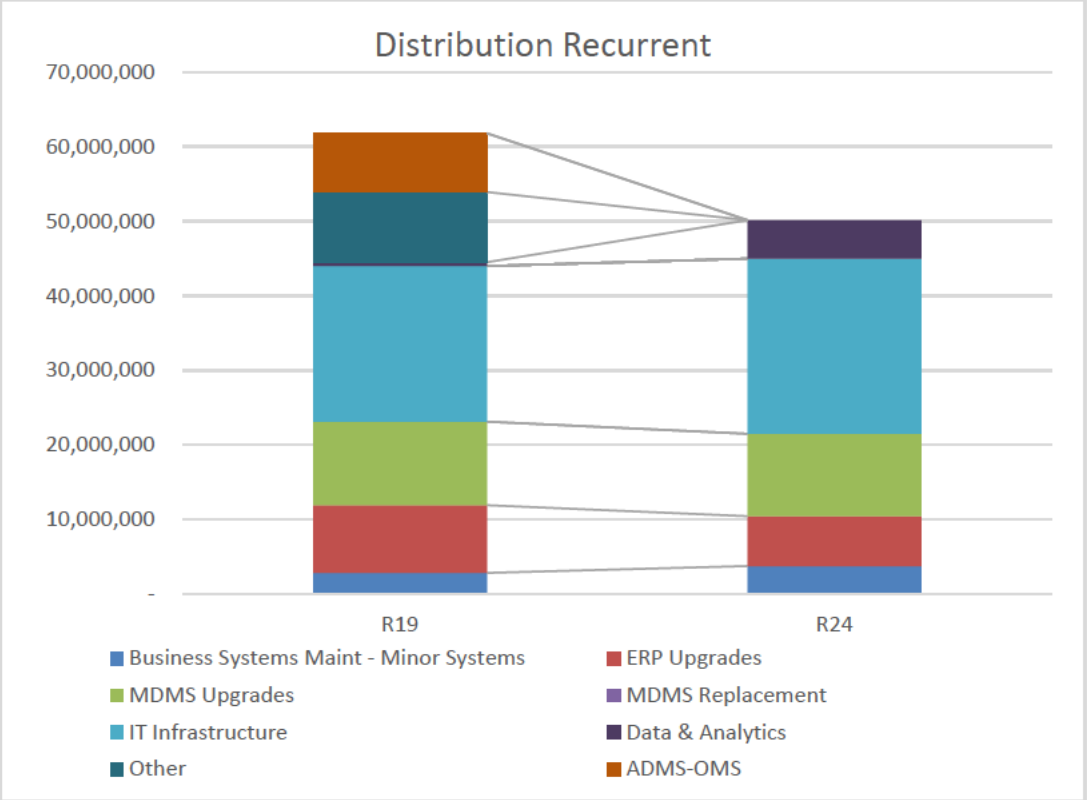
8.1.7 Distribution Recurrent Profile

The following information shows the Distribution Recurrent expenditure profile across the 2019-2024 and 2024-2029 regulatory control periods.

Table 12 – Distribution Recurrent profile across the 2019-2024 and 2024-2029 regulatory control periods.

Category	2019-2024	2024-2029
Business Systems Maint - Minor Systems	2,808,653	3,730,816
ERP Upgrades	9,085,020	6,689,557
MDMS Upgrades	11,212,800	11,055,881
IT Infrastructure	20,877,565	23,507,633
Data & Analytics	519,858	5,162,024
Other	9,418,163	-
ADMS-OMS	7,884,383	-
Totals	**61,806,441**	**50,145,911**

Figure 10 – Distribution Recurrent across the 2019-2024 and 2024-2029 regulatory control periods.



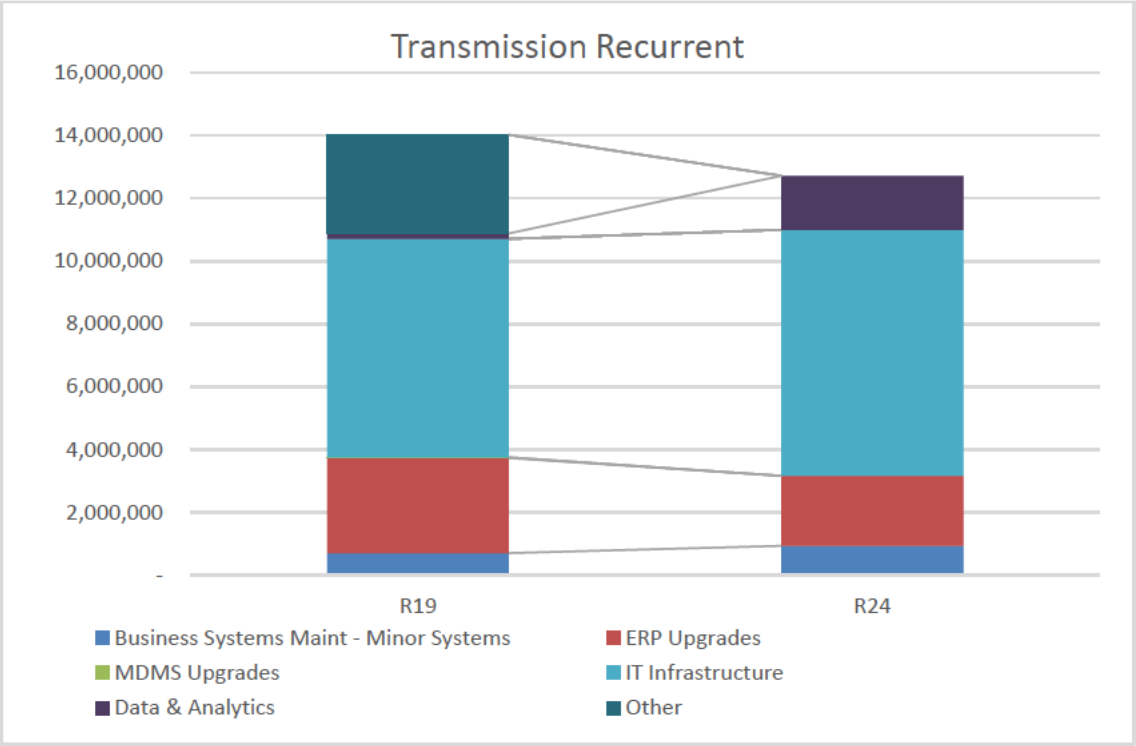
8.1.8 Transmission Recurrent Profile

The following information shows the Distribution Recurrent expenditure profile across the 2019-2024 and 2024-2029 regulatory control periods.

Table 13 – Transmission Recurrent profile across the 2019-2024 and 2024-2029 regulatory control periods.

Category	2019-2024	2024-2029
Business Systems Maint - Minor Systems	702,163	932,704
ERP Upgrades	3,028,340	2,229,853
MDMS Upgrades	21,152	-
IT Infrastructure	6,959,188	7,835,878
Data & Analytics	173,286	1,720,675
Other	3,139,388	-
Totals	**14,023,517**	**12,719,109**

Figure 11 – Transmission Recurrent across the 2019-2024 and 2024-2029 regulatory control periods.



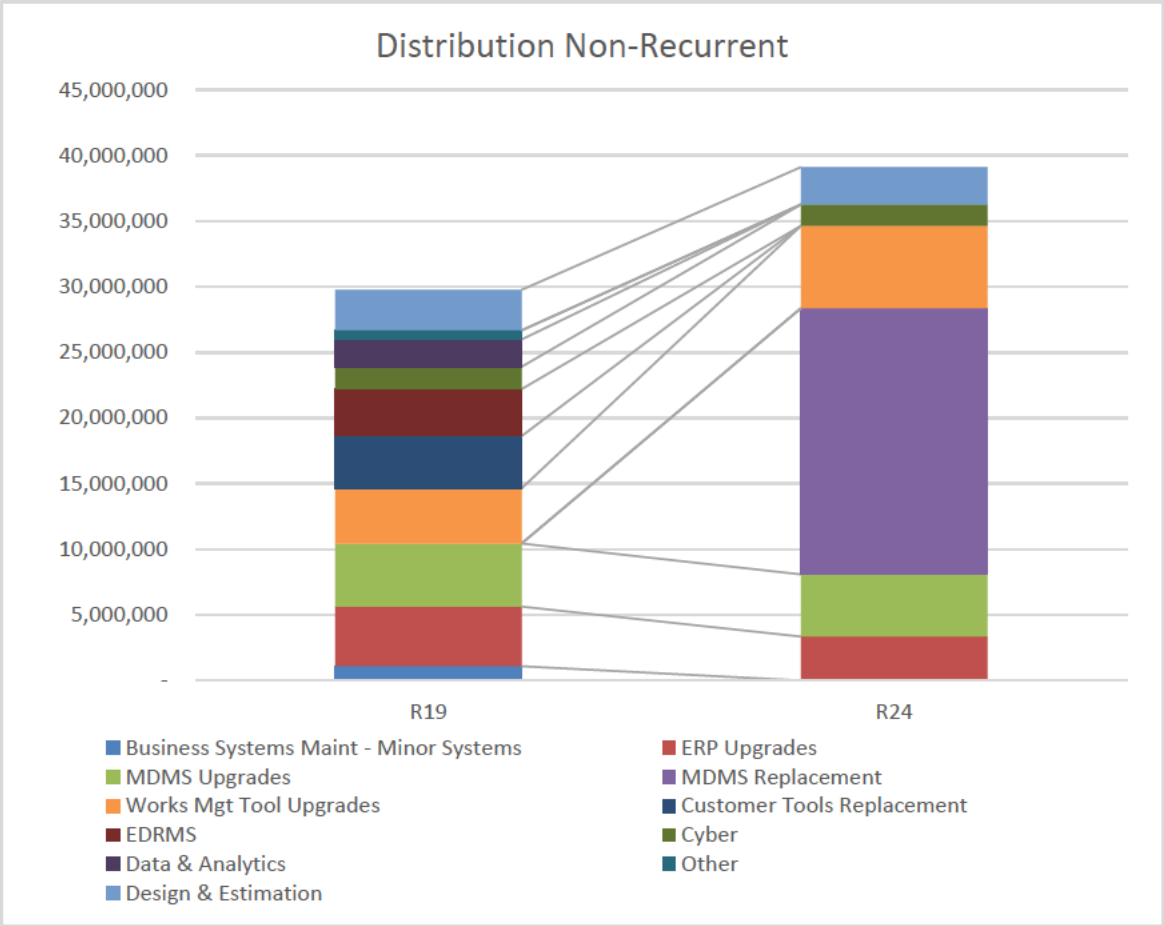
8.1.9 Distribution Non-Recurrent Profile

The following information shows the Distribution Non-Recurrent expenditure profile across the 2019-2024 and 2024-2029 regulatory control periods.

Table 14 – Distribution Non-Recurrent profile across the 2019-2024 and 2024-2029 regulatory control periods.

Category	2019-2024	2024-2029
Business Systems Maint - Minor Systems	1,086,218	-
ERP Upgrades	4,542,510	3,344,779
MDMS Upgrades	4,805,486	4,738,235
MDMS Replacement	-	20,275,253
Works Mgt Tool Upgrades	4,200,402	6,271,516
Customer Tools Replacement	3,979,162	-
EDRMS	3,577,631	-
Cyber	1,700,613	1,625,848
Data & Analytics	2,079,432	-
Other	693,200	-
Design & Estimation	3,087,353	2,847,234
	29,752,005	**39,102,865**

Figure 12 – Distribution Non-Recurrent across the 2019-2024 and 2024-2029 regulatory control periods.



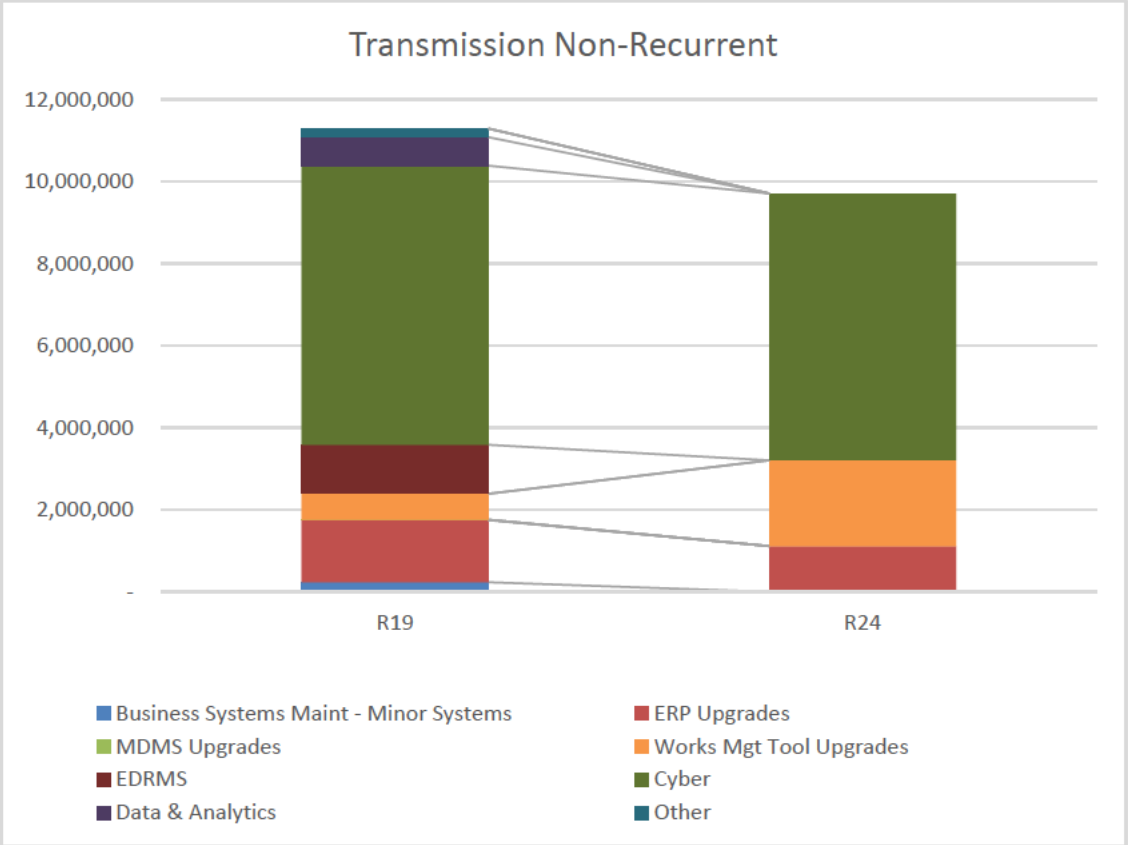
8.1.10 Transmission Non-Recurrent Profile

The following information shows the Transmission Non-Recurrent expenditure profile across the 2019-2024 and 2024-2029 regulatory control periods.

Table 15 – Transmission Non-Recurrent profile across the 2019-2024 and 2024-2029 regulatory control periods.

Category	2019-2024	2024-2029
Business Systems Maint - Minor Systems	234,054	-
ERP Upgrades	1,514,170	1,114,926
MDMS Upgrades	9,065	-
Works Mgt Tool Upgrades	633,467	2,090,505
EDRMS	1,192,544	-
Cyber	6,802,450	6,503,394
Data & Analytics	693,144	-
Other	210,800	-
Totals	**11,289,694**	**9,708,825**

Figure 13 – Transmission Non-Recurrent across R19 & R24



Distribution + Transmission Determination 2024-2029
Non-Network IT Application Roadmap

TasNetworks
Delivering your power

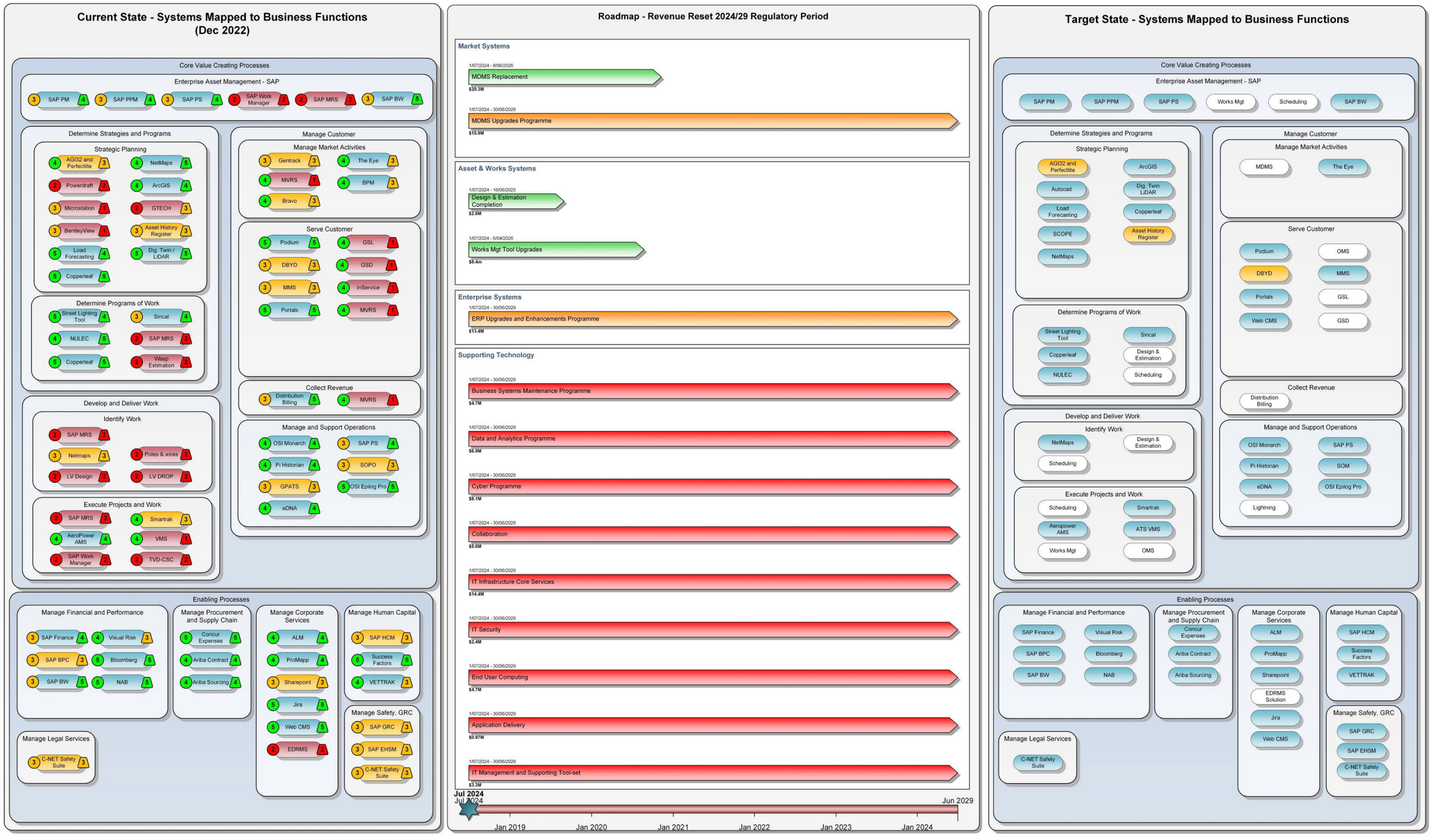


Figure 14 – 2024-2029 Predicted State of Core Applications