ICT Strategy

2017–2022

Department of Justice

Tasmanian Government

Version No.	Version Date	Description	Author	Approved By
0.1	1/11/2017	Initial Draft	M Lukianenko	
0.2	15/12/2017	Second Draft	M Hall	
0.3	2/2/2018	Formatted Draft	M Hall	
0.4	6/3/2018	Feedback from KMR	M Hall	

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

The Department of Justice has historically lacked a formal and holistic ICT strategy, and has not managed its ICT architecture at an enterprise level. This has resulted in a reactive and inconsistent approach to ICT investments, support and lifecycle management. In turn, this has resulted in the degradation of systems, increasing risk, creating barriers to innovation, and reducing the effectiveness and efficiency of IT as an enabler of business outcomes.

The 2017-2022 ICT Strategy is the result of an assessment of the current state of systems, people and processes, as well as a review of the strategic objectives of outputs across the Department, and its wider strategic context. The vision and intent is summarised in the diagram below.

VISION: That the department of justice has efficient and effective ICT services and solutions that are adaptive and trusted to deliver optimal business and customer outcomes.

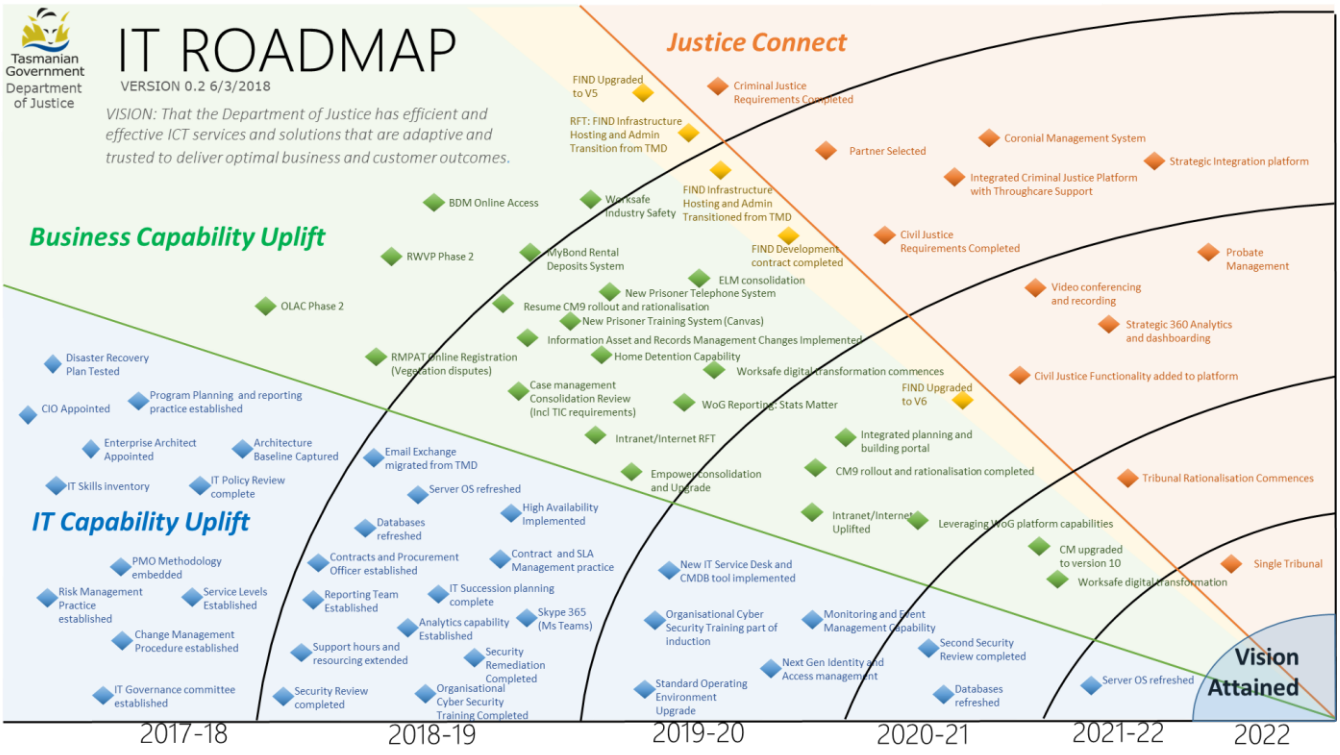
	Current State	Target State	Getting There	Benefits to Agency and Outputs
Systems	• No enterprise architecture • Siloed and aged solutions • Minimal integration • High manual effort • Lack of support 21% of systems are not formally supported • 40% of systems over 10 years old, some as old as 28 years	• ICT Architecture is managed as an enterprise • Fully supported and maintained systems • Systems are fit for purpose, easy to use and enable strategic outcomes • Systems integrate and automate business processes • Systems and data accessible and trusted	• Justice Connect • Business Improvement Roadmap • Enterprise Architecture Practices • System remediation plans • System maintenance plans	• Timely access to reliable information • Process efficiencies • Better service outcomes • Improved system supportability, availability and security • Reduced risk • Better agility to meet new changes • Increased functional capability
Technology	• Initial move to IaaS • Lack of tested disaster recovery and availability management • Lack of proactive technology refresh program • End of life technologies	• Technology is proactively managed and maintained	• ICT Maturity uplift Plan • Establishing service level and operational level agreements • ICT initiatives Roadmap	• Improved system availability • Reliable disaster recovery • Improved system security • Improved business agility • Able to respond to change • Quantifiable service levels
IT Service Capability	• Low maturity and lack of strategic planning • Reactive firefighting approach	• Established and mature processes and KPIs • Trusted to deliver • Continuous improvement in place	• ICT Maturity uplift Plan • Establishing service level and operational level agreements	• ICT Services able to meet business demand • Trusted business partner • Agreed turn-around times
IT Delivery Model and Governance	• Lack of overall governance and planning • 53% of systems with support key person dependencies	• Centralised investment governance • Centralised support and delivery model eliminates Key Person Dependency risks and unlocks economies of scale	• ICT Governance initiatives • ICT Maturity uplift Plan • Transition to centralized support model	• Reduced operational risk • Ability to focus on core business • Better IT outcomes through economies of scale

This target state vision will be achieved by meeting the strategic objectives listed below. The objectives will be implemented through a roadmap of initiatives, and governed by a set of defined principles. These are further elucidated throughout this document.

The key objectives of this strategy are:

- Reducing Complexity
- Improving operational efficiencies and effectiveness
- Enabling operational innovation and agility
- Improving security and reliability
- Maturing vendor and contract management

Initiatives will focus both on solution outcomes for the department and uplifting the ICT service capability and maturity. The initiatives roadmap is encapsulated in the diagram below:



This roadmap represents significant but long overdue investment in ICT for the Department, and the benefits are expected to flow to other agencies and the wider Tasmanian community.

2 INTRODUCTION

The Information and Communication Technology (ICT) Strategy has been developed in support of the Department of Justice's vision of 'ensuring an effective, efficient and accessible justice system'. The ICT Strategy also supports and aligns with the Corporate Support and Strategy Business Plan by ensuring that the Agency is in a position to deliver fit for purpose solutions while focussing on operating efficiencies and customer engagement.

The primary focus of the Strategy is to deliver quality services that enable the Agency to meet its objectives as a whole, and this is a consideration in every aspect of the decisions, delivery, and initiatives undertaken. The aim of the Strategy is to ensure that the utilisation of technology is adopted to deliver the productivity and automation that the organisation will rely on to operate effectively and efficiently. As such, the objective of the Strategy is to position our systems and processes to maximise value to the community and Agency clients.

2.1 Business Context

The Department of Justice encapsulates a diverse number of delivery outputs ranging from administration of justice, legal services, corrections, enforcement and consumer protection, as well as regulatory services. These functions are often completely unrelated to each other and serve as separate business entities in regards to their ICT requirements.

In addition, the Agency supports a number of independent statutory authorities with varying levels of management autonomy. The Agency provides ICT services to these on a case-by-case basis, with some opting to manage their own ICT support functions.

There are a number of vital external and stakeholder interactions and dependencies including the Tasmania Police Service, Department of Health and Human Service, Office of e-Government, as well as Department of Premier and Cabinet. All of these rely on the secure, timely exchange of quality information, underpinned by a robust ICT capability.

The Agency serves a diverse public customer base with interactions relating to significant life matters, often with financial, safety and personal security implications. These interactions are occurring in a context of increasing customer expectations for information delivery and engagement (e.g. digital, timely information, self-service), increased security and reputational risk (cyber security, social media sharing), and increased media and public scrutiny. In addition,

changes to legislation will have impacts on scalability and place pressure on some existing systems and processes.[1]

In other jurisdictions, Departments of Justice are moving to implement increased digital engagement opportunities and enhanced integration between justice administration systems. This includes Western Australia, South Australia, Victoria and New South Wales. In addition, federal agencies such as the Federal Police and Intelligence community are increasing the use of 'big data analytics' to ensure strategic protection of the public, and there are increasing expectations for information sharing, transparency and consistency. These expectations also bring an increased requirement for information classification and security.

The Tasmanian Office of e-Government is currently developing a *Strategy for Digital Innovation* with a vision and set of objectives that will impact all government departments. This strategy is supported by a State Government funding allocation of $60M for digital transformation across the state. There are also other opportunities arising from Federal Government initiatives such as the Cutting Red Tape initiative.

As a Government Department, the political context (including state and national) sets the competing expectations of agility to respond to change and risk-averse prudence. Being linked to election cycles brings with it a number of challenges including investment cycle alignment and prioritisation against other departments, and managing reputational and brand risk— not only for the Agency, but also supporting the Government. Other states are already attempting to increase transparency and accountability for large IT projects through the use of public dashboards.[2]

2.2 Methodology

Fundamentally, ICT is an enabler of business strategy and business outcomes. This is realised best when the technology capabilities align to organisational goals and processes, and when the technology remains up to date and able to respond to new requirements. Knowledge of the organisational strategy and direction must be understood in the context of the current system capability and constraints.

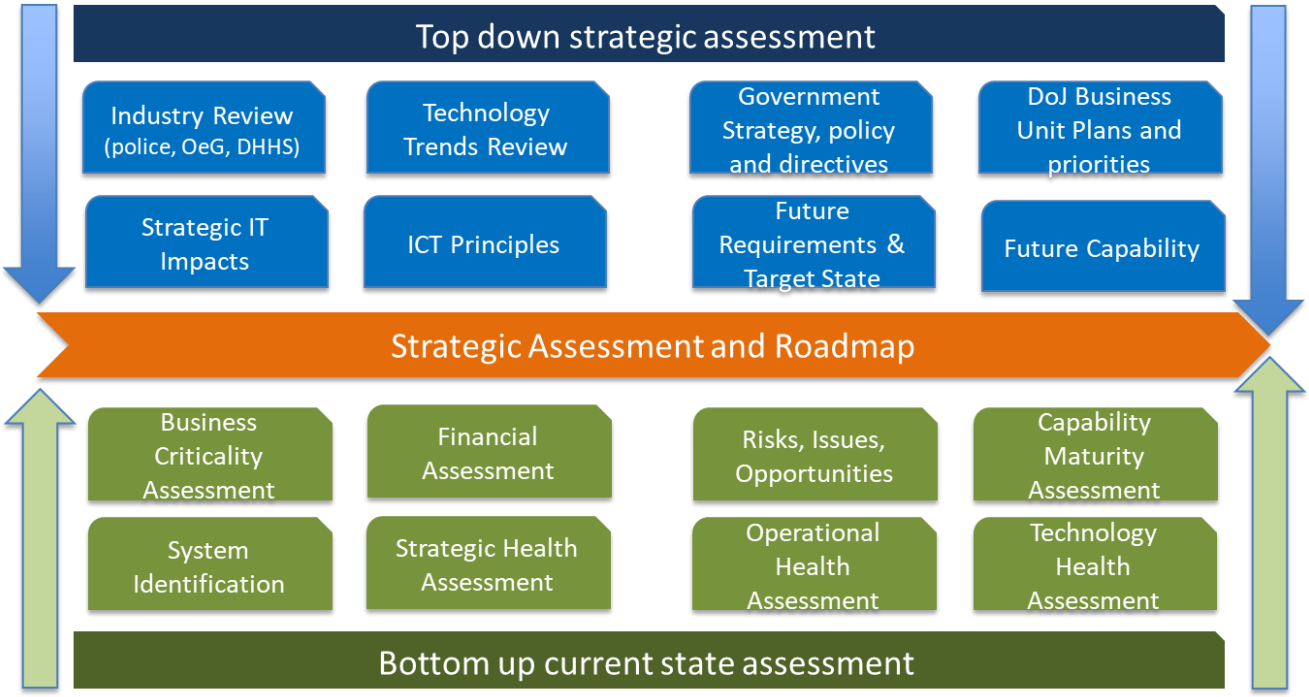
As such, the ICT Strategy has been developed from two viewpoints:

1. A top-down assessment of the strategic objectives and external change factors; and
2. A bottom-up assessment of the current health of all the ICT systems and ICT management capability, from an operational business use view of health, as well as a technology health profile.

[1] As an example, it is expected that the number of prisoners in the state will increase from approximately 600 to 1,100 by 2029-30 due to average growth rates and policy changes.
[2] For example, Victoria's ICT dashboard: https://www.enterprisesolutions.vic.gov.au/ict-dashboard/ , and New South Wales: https://www.digital.nsw.gov.au/

The bottom up assessment creates a baseline view of system health, highlighting areas of strength and weakness that can be leveraged or must be overcome in order to enable the strategic initiatives to succeed. The top-down assessment ensures that the IT vision aligns with the Agency's business plans and objectives.

Scope and activities for each line of enquiry undertaken are depicted in the diagram below:

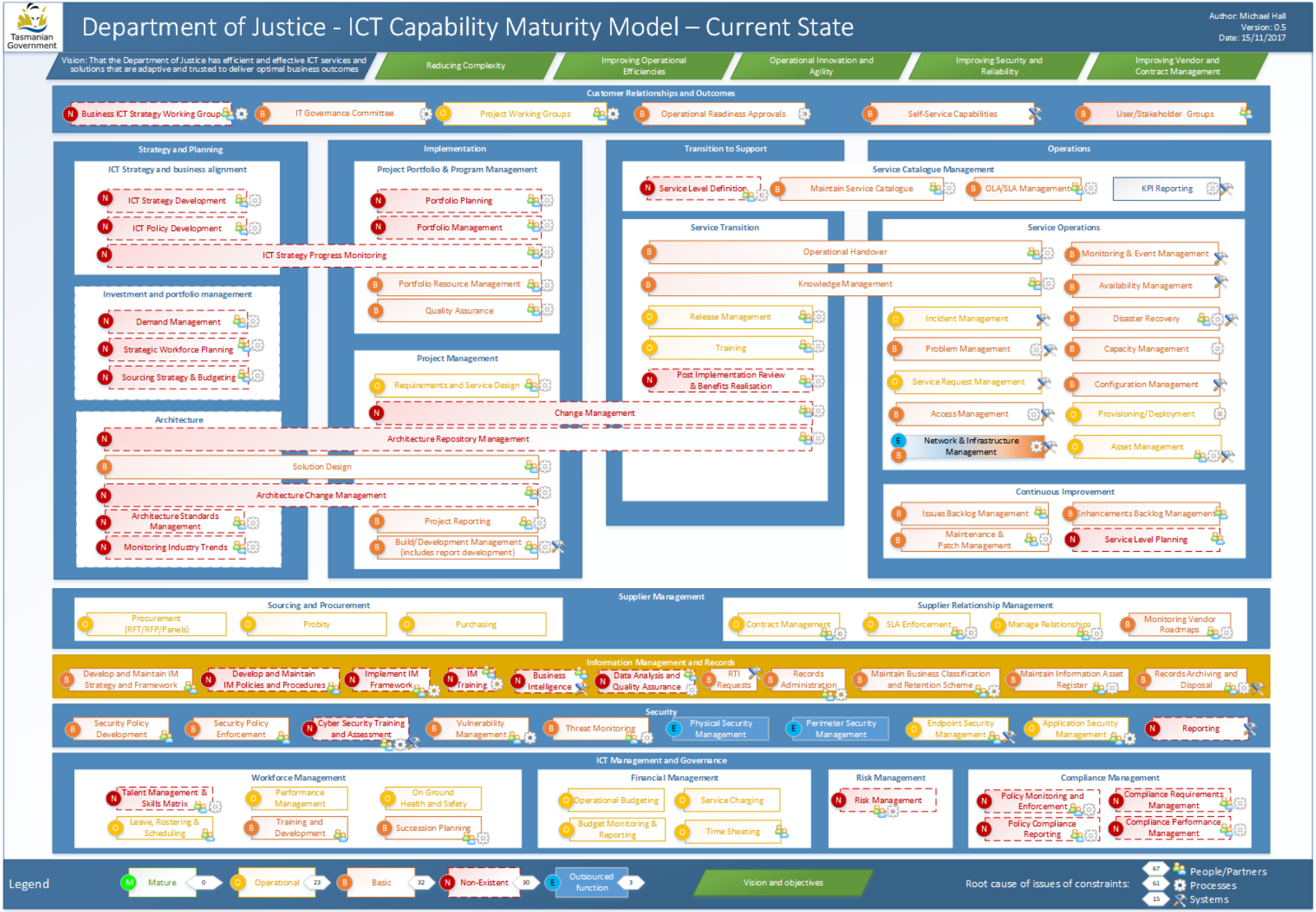


The assessment process was conducted over ten weeks in late 2017, and included interviews with output managers, key system users, the ICT and Projects and Information Teams, and external parties such as Tasmania Police, and the Office of e-Government. In addition to interviews, technical and financial information was obtained and analysed for systems, and information sought from software vendors. A desktop review of all business unit plans was also undertaken to identify future directions and their impacts to ICT. A high-level review of Justice Departments in other Australian jurisdictions was also conducted, together with a sweep of general ICT trends and emerging technologies.

2.3 Current Issues

Against this context the bottom up assessment has found a chronic underfunding of investment in ICT initiatives and capabilities that has accumulated a significant backlog, or 'technical debt'. This has increased current operational and strategic risk and also remediation complexity and effort. The remediation backlog, in turn, creates a barrier to further innovation since many of the current systems cannot be adapted to meet new requirements.

The investment gap is not limited to the systems themselves, but also includes a lack of support resources and skills. This has resulted in a number of key ICT management capabilities which have no ownership and as such are currently non-existent. The ICT capability maturity level for the Agency is low across the board and ICT standards cannot be adequately maintained, as depicted in the capability maturity assessment below:


Department of Justice - ICT Capability Maturity Model – Current State
Author: Michael Hall
Version: 0.5
Date: 15/11/2017
Vision: That the Department of Justice has efficient and effective ICT services and solutions that are adaptive and trusted to deliver optimal business outcomes
Reducing Complexity
Improving Operational Efficiencies
Operational Innovation and Agility
Improving Security and Reliability
Improving Vendor and Contract Management
Customer Relationships and Outcomes
Business ICT Strategy Working Group
IT Governance Committee
Project Working Groups
Operational Readiness Approvals
Self-Service Capabilities
User/Stakeholder Groups
Strategy and Planning
ICT Strategy and business alignment
ICT Strategy Development
ICT Policy Development
ICT Strategy Progress Monitoring
Investment and portfolio management
Demand Management
Strategic Workforce Planning
Sourcing Strategy & Budgeting
Architecture
Architecture Repository Management
Solution Design
Architecture Change Management
Architecture Standards Management
Monitoring Industry Trends
Implementation
Project Portfolio & Program Management
Portfolio Planning
Portfolio Management
Portfolio Resource Management
Quality Assurance
Project Management
Requirements and Service Design
Change Management
Project Reporting
Build/ Development Management (includes report development)
Transition to Support
Service Transition
Operational Handover
Knowledge Management
Release Management
Training
Post Implementation Review & Benefits Realisation
Operations
Service Catalogue Management
Service Level Definition
Maintain Service Catalogue
OLA/SLA Management
KPI Reporting
Service Operations
Monitoring & Event Management
Availability Management
Incident Management
Disaster Recovery
Problem Management
Capacity Management
Service Request Management
Configuration Management
Access Management
Provisioning/Deployment
Network & Infrastructure Management
Asset Management
Continuous Improvement
Issues Backlog Management
Enhancements Backlog Management
Maintenance & Patch Management
Service Level Planning
Supplier Management
Sourcing and Procurement
Procurement (RFT/RFP/Panels)
Probity
Purchasing
Supplier Relationship Management
Contract Management
SLA Enforcement
Manage Relationships
Monitoring Vendor Roadmaps
Information Management and Records
Develop and Maintain IM Strategy and Framework
Develop and Maintain IM Policies and Procedures
Implement IM Framework
IM Training
Business Intelligence
Data Analysis and Quality Assurance
RTI Requests
Records Administration
Maintain Business Classification and Retention Scheme
Maintain Information Asset Register
Records Archiving and Disposal
Security
Security Policy Development
Security Policy Enforcement
Cyber Security Training and Assessment
Vulnerability Management
Threat Monitoring
Physical Security Management
Perimeter Security Management
Endpoint Security Management
Application Security Management
Reporting
ICT Management and Governance
Workforce Management
Talent Management & Skills Matrix
Performance Management
On Ground Health and Safety
Leave, Rostering & Scheduling
Training and Development
Succession Planning
Financial Management
Operational Budgeting
Service Charging
Budget Monitoring & Reporting
Time Sheeting
Risk Management
Risk Management
Compliance Management
Policy Monitoring and Enforcement
Compliance Requirements Management
Policy Compliance Reporting
Compliance Performance Management
Legend
Mature
Operational
Basic
Non-Existent
Outsourced function
Vision and objectives
Root cause of issues of constraints:
People/Partners
Processes
Systems

The capability gaps in the areas of strategy, planning, architecture and project portfolio management result in a highly reactive posture for the ICT team who are, in turn, unable to deliver to the expectations of the Agency and its outputs.

As a result of the low capability and capacity, broadly speaking, individual business outputs have tended to work around the ICT support service to implement and support their own solutions. While this approach has enabled some outputs to achieve outcomes they otherwise would have foregone, it has led to a number of issues:

- Solutions are often siloed, resulting in duplication of systems and data. As an example there are 14 case management systems within the Department, and multiple records management systems.
- Solutions are not always well designed, resulting in:
    - a high number of manual work-arounds;
    - security vulnerabilities;
    - inadequate availability and disaster recovery capabilities; and
    - inadequate performance and scalability.
- Solutions are not integrated, resulting in increased duplication of manual effort. This is a particular pain point within the criminal justice functionality where information is often printed out of one system and re-keyed into another system.
- The majority of solutions are not well documented, and are supported on the side of people's desks resulting in:
    - key person dependency risks for 53% of systems;
    - reactive support models;
    - increasing issue backlogs;
    - data integrity issues; and
    - compromised ability to support the system overall.
- Solutions are not holistically funded for their full life cycle (e.g. OPGuard), resulting in:
    - inability to assign adequate internal support resourcing;

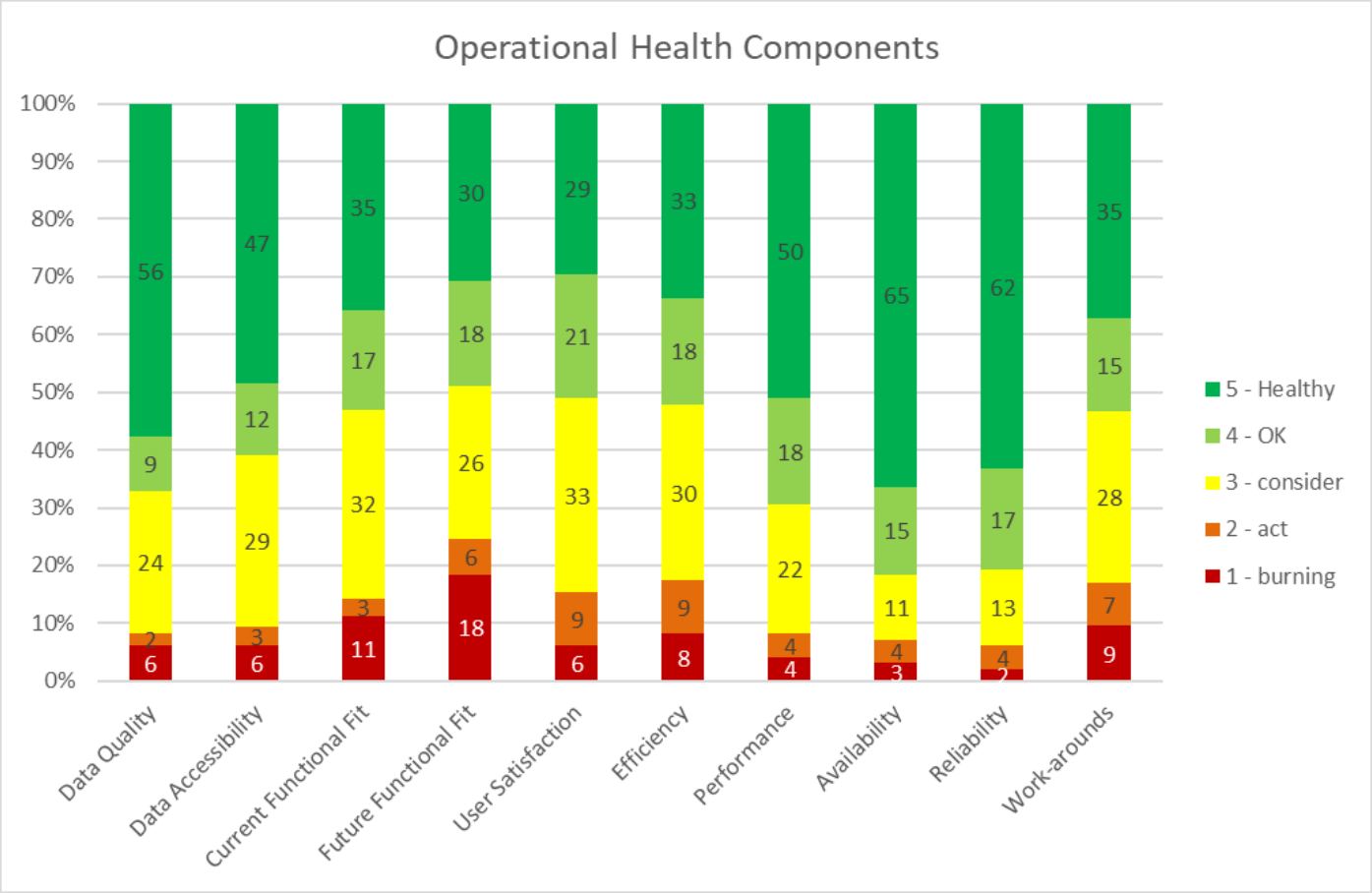
- 21% of systems lacking ongoing vendor support including 17% of business critical systems (increasing operational risk);
- 40% of business critical systems are over 10 years old, and there are some systems that are as old as 28 years; and
- inability to adapt the system to changing requirements.

The accumulation of these issues over the years has led to a portfolio of systems in declining health that are not serving business needs effectively and carry high operational and strategic risk. Added to this risk is a relatively common lack of disaster recovery and business continuity plans. As an example, the current restoration time for the Births Deaths and Marriages register, Vitalware, is estimated to be 30 hours based on restoring 7TB of data.

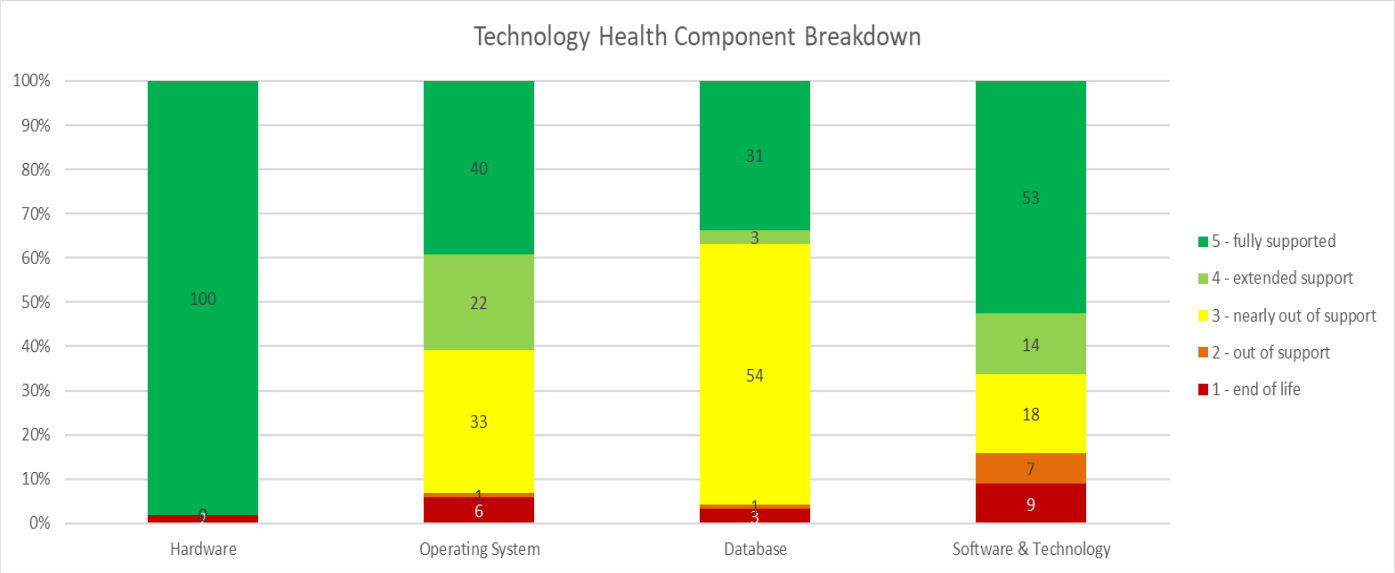
The final outworking of this scenario is that the quality of data is not sufficient to support critical processes, and there have been a number of issues that have drawn negative media and Government attention.[3] Independent reviews into these issues have consistently pointed to underlying gaps in system processes that lead to a high reliance on key people to enter and re-enter information correctly into multiple repositories.

System Health metrics are included below:

[3] For example two external reviews into the court processes for remand and sentencing were conducted, one by KPMG and one by Tempus. Each report found excessive duplication of manual data entry due to system and integration limitations.



The proportion of high work-around, low efficiency systems depicted above is a function of degrading functional fit and inability to adapt functionality to changing business needs over time due to the lack of ongoing maintenance and support. This in turn leads to lower user efficiency and poor data quality. The chart below illustrates that the issue is about to get worse in relation to database and operating system support, which is about to end on a large proportion of systems, while there are a number of end of life technologies impeding future upgrades.



These technology and operational health issues are the result of an inappropriate funding and support model. It is noted that the current operating model is well entrenched, and it will be difficult to change to a well-managed centralised delivery and support model without first uplifting the capability and capacity of the ICT service to make it an appealing value proposition to respective outputs and independent statutory authorities.

2.4 Drivers

From the business context and current issues a number of drivers have been identified that inform the vision and strategy for ICT in the Agency:

1. The need to ensure robust and secure ICT solutions
2. The need to ensure that ICT enables efficient and effective business outcomes
3. The need for better information integration and sharing
4. The need to adapt to rapidly increasing external requirements
5. The need to meet increasing customer and stakeholder expectations
6. The need to holistically and strategically manage the ICT portfolio

3 ICT VISION

The vision that encapsulates this strategy is:

> *That the Department of Justice has efficient and effective ICT services and solutions that are adaptive and trusted to deliver optimal business and customer outcomes.*

This vision is in line with the overall vision of the Department for 'a safe, fair and just Tasmania' by directly aligning to the corporate vision of 'ensuring an effective, efficient and accessible justice system'.

4 ICT GUIDING PRINCIPLES

The following principles will be applied to investment decisions and solution selection:

ICT investment will be…

1. Strategically Aligned ICT decisions will be aligned with Agency objectives and strategy as opposed to siloed outcomes, while at the same time acknowledging the specific requirements of outputs and independent statutory authorities.
2. Holistically Managed Change will be managed at the systems, organisation and Agency level as a whole.
3. Demonstrably Beneficial ICT decisions will have clearly defined business outcomes, customer benefits, be commercially prudent, coupled with a strong risk management focus.

ICT Solutions will be…

4. Optimally Architected Current systems and new solution proposals will seek to reduce diversity and complexity of technology and architecture; with the intent to digitise/automate.
5. Partnership Delivered Strategic alliances and partnerships will be utilised where possible to increase capability and maturity; leveraging Whole of Government initiatives where practical.
6. Robustly Supported ICT systems and infrastructure will be secure and supported, underpinned by defined service levels and robust contracts.

Outcome…

That Department of Justice has efficient and effective ICT services and solutions that are adaptive and trusted to deliver optimal business and customer outcomes.

5 ICT STRATEGY ALIGNMENT – ENABLING STRATEGIC OUTCOMES

A review of Agency objectives and individual output business unit plans has been conducted to inform this Strategy and ensure it aligns with and enables the Agency to meet its holistic and output specific outcomes. Given the number and diversity of business unit plans reviewed, the results have been distilled to a number of key strategic ICT outcomes:

- Optimal operations and efficient processes
- Trusted service provider
- Trusted , timely, meaningful and accessible data
- Digitisation of customer engagement and business processes
- Improved Access to ICT – Data, Mobility and Collaboration
- Reduced Complexity
- Better End User Experience

In order to achieve these outcomes it is critical that the focus for ICT is to deliver systems and process that align to the broader Agency outcomes. The following table represents the ICT alignment to these:

Theme	ICT Implications
Digitisation of customer engagement	• User Experience (UX) led design • Support electronic forms lodgement and workflows • Support integration of forms to systems and feedback channels • Online chat, forums, information sharing • Video conferencing enabling public and Agency interactions • Multiple digital channels (e.g. apps, IVR, SMS, video chat) • Customer self-service

Efficient and effective business processes	• Business process improvement – consistency, efficiency… • Business process automation • Business rule enforcement • Reduce wasted effort through business rule and data validation • Maximise system efficiency through system maintenance and performance tuning • Reporting that supports operations and strategic decisions • Data quality management • Mobility and field tools
Accessible IT	• Plain English program • Support for people with disabilities • Workforce Diversity and inclusion Policy • BYOD and mobile • Training and support • 24/7 channels preferred over physical B/H offices
Collaboration and integration	• Automation of data flows between systems and processes • Transparency of information • Information sharing with external stakeholders
Web channel enhancements	• User Experience (UX) led design • Enhanced web capabilities • Contemporary look and feel • Better content to support user needs
Reporting and Analytics	• Improved ability to analyse and report on data • Underpinned by better data capture and quality controls
Records Management	• Move to digital records management (e.g. CM9) • Records disposal and archiving
Risk management	• Improved availability and disaster recovery capabilities • Data quality management and assurance • Reduce key person dependencies • Systems are reliable, available, robust, resilient, and perform • Data quality is maintained • Vendor contracts are well managed and ensure adequate protection • Internal SME knowledge is shared and documented as appropriate, with no single person dependencies • Appropriate system environment security controls in place
Security	• Increased requirements for security, from policy to incident management
Strategic planning	• Strategic system and asset lifecycle management • Agility to respond to new requirements • Forward planning and prioritisation
Rationalisation	• Reduce complexity of environment by reducing multiple redundant technologies and rationalising systems where appropriate

Financial model	• Ensure IT investment model facilitates whole of life system and asset management • Portfolio-wide funding view • Project prioritisation mechanisms • Cost-reflective modelling • Centralised ICT to increase economies of scale and reduce KPD
Vendor and Contract management	• ICT Contract review and renegotiation • Vendor consolidation • Reduced system downtime through better monitoring and support • Faster service request turn around • Process efficiencies • Optimised system maintenance profile • Efficient use of operational and project resources (resource planning) • Reducing ICT support costs through better design and implementation (clear requirements). Supporting business process automation

5.1 Alignment to Relevant External Agency Strategies

In addition to reviewing the business plans of the department's outputs, consideration has been given to the Office of e-Gov *Strategy for Digital Innovation*, and also the strategic Tasmania Police Service's *Project Unify*, since these will have strategic influence the ICT strategy. It is noted that there is no current approved whole of government ICT strategy to reference.

Stakeholder	Vision	Key Themes and Objectives	Implications for ICT
DPAC – OeG	To deliver better services for all Tasmanians by transforming the way in which the Tasmanian Government values, manages and shares information and technology	• Increase options available for people to connect and interact with Government, when and how they want, irrespective of age, gender, location, ability, life circumstances or cultural heritage. • One government – one organisation – one client • We need to support government employees to work better together to	• Online, integrated systems supported by robust, flexible and fit for purpose reporting • Standardised look and feel across Government • Consistent user experience across Government • Integration to national identity management services • Potential restructure of IT service delivery model across and between agencies, as well as future of TMD

Stakeholder	Vision	Key Themes and Objectives	Implications for ICT
		improve technology and internal processes. • We need to help agencies to work in new ways and collaborate more effectively to deliver better outcomes.	• Whole of government digital initiatives, platforms and standards: ○ SMS ○ Forms ○ Web ○ Collaboration and communication technologies ○ Cybersecurity ○ Information Management classification and integration
Tasmania Police Service	Project Unify	• Replacement of legacy systems with an integrated management system	• Impacts to Justice Connect program

6 OBJECTIVES

Whilst the guiding principles of the ICT strategy provide a decision-making framework, it is the objectives that define the intent and purpose of the strategy to realise the benefits expected. This section outlines the broad objectives of the strategic approach.

6.1 Reducing complexity

The current application and technology landscape has 'organically evolved' over an extended period of time, caused by siloed solution and decision making, where a decentralised model has been adopted. This has resulted in an environment where many applications do not integrate with each other and are not well understood, inhibiting the ability to make holistic strategic longer-term decisions. There is a:

- High functional overlap;
- manual point to point integration that has organically evolved without strategic planning; and
- multiple technology stacks, which adds to the complexity of support.

Resources and new disciplines are required to facilitate rationalisation of existing systems and technologies used as well as planning and proactive designing of new systems to ensure optimal investment outcomes from an Agency-wide perspective.

6.2 Improving operational efficiencies and effectiveness

Adopting the "out-of-the-box" best practice processes encapsulated in good off the shelf applications speeds up operational efficiency. The efficiencies realised through the adoption of good practice processes and adopting 'vanilla' functionality supports the strategic objective of minimising the cost to customers. Any customisation of processes needs to be scrutinised to ensure they add value or fulfil a mandatory legal requirement, as customisations add not only to the original implementation cost but also to the ongoing maintenance and upgrade costs and complexity of the system.

By ensuring processes and systems align to the strategic objectives and ensuring each process adds value, the likely gains are:

- cost reduction through improved effectiveness and productivity;
- end to end operational efficiencies resulting in improved service quality; and
- proactive planning and support.

Additional value can be unlocked by introducing new processes within ICT projects to ensure better knowledge transfer to support, better ongoing risk management and whole of lifecycle management planning for systems is factored in.

6.3 Enabling operational innovation and agility

It is imperative that we are in a position that we can readily adapt to changes given the evolving and changing societal needs.

New digital customer and end user engagement channels will be required along with the flexibility to adapt with community requirements. Current systems are typically from earlier generation architectures and are not as open to supporting agility, digital customer engagement and open integration. The strategy for these systems will consider whether they can be augmented by new middleware and presentation layers, or whether new systems are required to position the Agency for current and future engagement needs. An assessment of currently manual or paper based interactions with public and external customers is also required to ensure improved outcomes.

The benefits of such innovation extend both to the customers and to internal staff efficiency and effectiveness:

- Customers can make applications at any time of day from the convenience of their home or office;

- information is entered once, and re-used;
- business logic and process is automated and streamlined where possible;
- turn-around times for customers are reduced; and
- information is available and accessible at any time of day.

6.4 Improving security and reliability

With an increased customer facing digital footprint, availability, reliability and performance become vital. This also becomes important for systems replacing currently manual processes in the court, which cannot afford extended outages. The ability to define service levels and then monitor and measure performance to those service levels will improve customer satisfaction and business performance, as well as facilitating future planning and decision-making.

Ensuring that robust ICT governance controls are in place, monitored and continuously assessed against good practice will be critical for the success and protection of the Agency data and assets.

Ensuring that appropriate disaster recovery of core applications and technologies, along with business continuity procedures and processes are in place and tested on an annual basis will also become a fundamental requirement to support the security and reliability of the system.

Monitoring emerging trends in cyber security risks, network penetration, vulnerabilities and customer privacy will also be essential. This also includes uplifting cyber security awareness and vigilance for all staff members.

6.5 Maturing vendor and contract management

Ensuring vendor contracts have defined service levels aligned to business success factors will enable the Agency to safeguard system effectiveness, efficiency and availability. In addition to the quality of the contracts, active management of vendors and contracts, including regular scheduled reviews and vendor relationship and performance management is crucial to maximise the value of ICT investments, and will contribute to strategic planning and development. This function is currently applied inconsistently across systems and in many cases there is no active management of contracts or vendors, leading to system degradation over time and a loss of leverage to mitigate the issues.

An uplift of vendor and contract management capability will be achieved though:

- Sourcing arrangements that best-fit the needs of the Agency;

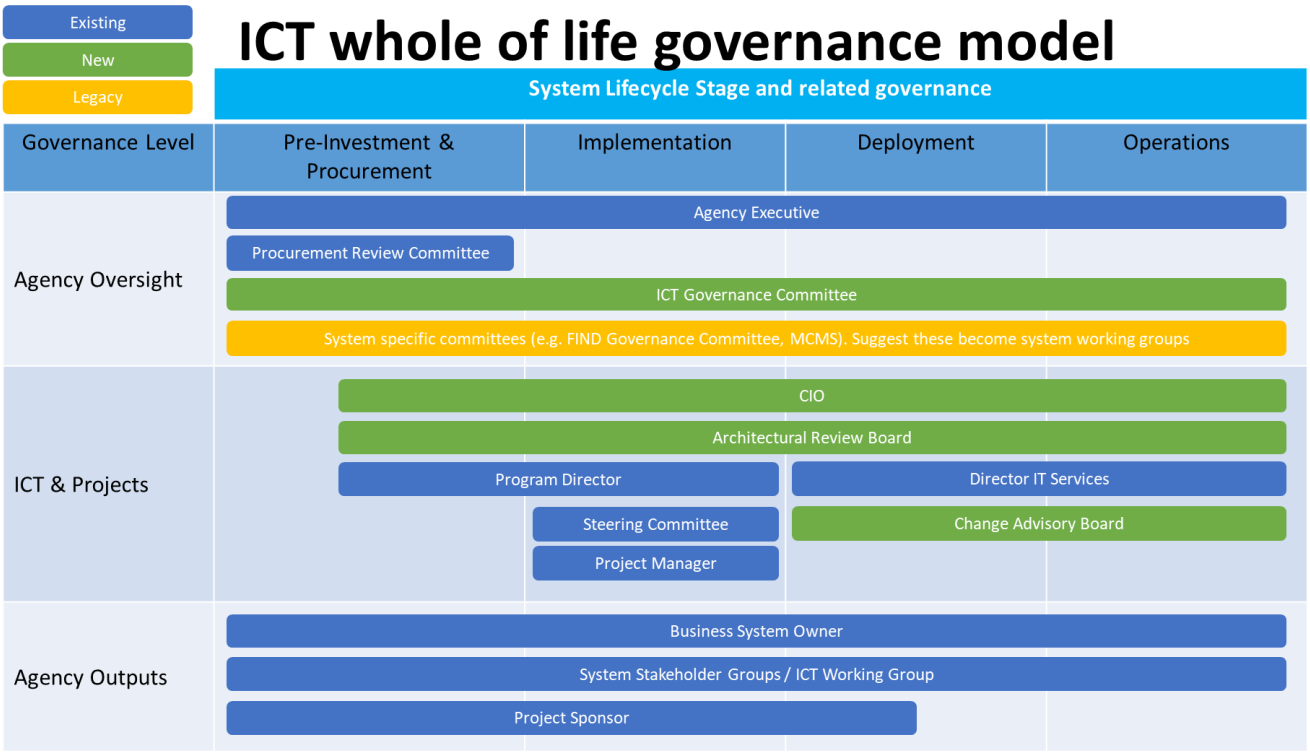
- Overall ICT budgetary ownership and transparency;
- Proactive management of vendors, their capabilities, performance, costs and strategic importance;
- Service Levels being defined, monitored and managed; and
- Understanding the cost of IT through development of a future IT funding model.

To ensure that the services are both cost effective and efficient, a focus will be placed on forming more strategic alliances and consolidating relationships and agreements with vendors. Ensuring that strategic partners are selected for their expertise and known delivery will be key. Enhancing our contracts to ensure they deliver to expected business outcomes will also be a key factor to success.

7 ICT GOVERNANCE

It is imperative that ICT decisions and initiatives are understood and appropriately governed, not only at inception but ongoing to ensure that whole of Agency strategic objectives, priorities and risks are considered.

A number of new governance structures will be put in place to achieve this goal.



The ICT Governance Committee will be responsible for:

- Developing and maintaining a multi-year strategic ICT plan and roadmap, along with an annual ICT work program to help guide ICT investments across Agency;
- Maintaining ICT governance and oversight, which includes guiding all ICT investment, approving all ICT standards, monitoring ICT performance and ensuring ICT initiatives are aligned with strategic business objectives;
- Endorsing and Approving information and technology policies for the agency;
- Establish business planning principles and processes to be applied to new information and technology investments, including business case development and approvals;
- Considering and promoting opportunities for Agency-wide or WoG enterprise ICT business initiatives;
- Seeking funding allocation for required initiatives and projects as necessary;
- Overseeing the Agency's corporate information and technology budget and major information and technology project progress and initiatives; and
- Communicating ICT activities and decisions across the Department.

The ICT Working Group will be responsible for:

- Inputting requirements and business objectives into strategic ICT goals;
- developing ICT policies;
- prioritisation of business ICT needs; and
- championing business output engagement and ICT ownership.

The Architectural Review Board will be responsible for:

- Solution alignment to enterprise architecture, IT principles and strategy;
- independent solution quality assessment;
- project interdependencies assessment;
- architectural impact assessments;
- architecture component re-use possibilities; and
- defining and enforcing architectural standards.

The Change Advisory Board will be responsible for ensuring all changes to production systems are:

- Managed (deployment plans, run sheets, rollback planning);
- appropriately tested and system ready for go live;
- operationally ready for go live (training, communications, resource allocation); and
- supported, ready for go live (training, knowledge transfer and documentation).

It is acknowledged that there are additional governance mechanisms that will remain in place, including the FIND governance committee, and the procurement review committee.

In addition to governance structures, a full review of Agency ICT policies and their underlying implementation and enforcement procedures is required.

8 ARCHITECTURE

The practice of enterprise architecture exists to ensure that ICT investment and delivery supports Agency strategy and delivers optimum outcomes across the business. Its goal is to mitigate the proliferation of disparate, siloed solutions and duplication of process and data by applying a 'big picture' lens across the entire enterprise. It understands the overarching direction and requirements and therefore how silos of requirements integrate with the whole. This information is used to inform planning, problem solving and decision-making to facilitate investment that is demonstrated to align to the organisational objectives and strategy. Enterprise architecture includes the following functions:

- Strategic planning
    - External environment reviews and trends analysis
    - IT road-mapping
- Architectural governance
    - Impact assessments
    - Architectural review and change management
    - Technical design authority
- Architectural standards management and enforcement
    - Security
    - Integration and interoperability
    - IT Best practices
- Solution design
    - Conceptual Design
    - Solution Design
- Architecture repository management
    - Process architecture repository

- Systems architecture repository
- Data architecture repository
- Integration architecture repository

- Technology reference model management
  - Reduce technology proliferation
  - Reduce complexity
  - Ensure supported technologies with future roadmaps are adopted

The current state within the Agency is that there is no enterprise architecture capability.[4] Investment in this capability will be crucial to ensure ICT can continue to delivery in a highly integrated, digital environment, and break free from a reactive posture.

9 SERVICE DELIVERY MODEL

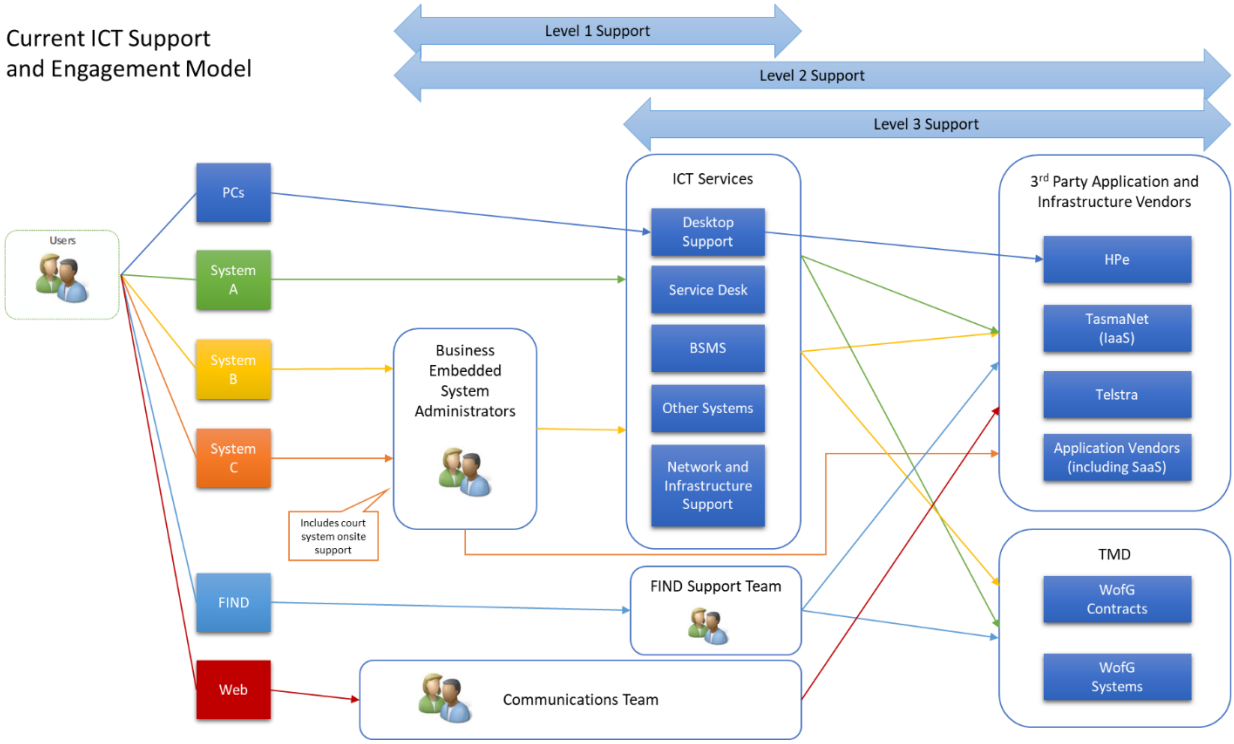
9.1 Current state

The current ICT service delivery model is a hybrid between a federated model with embedded IT management within business outputs, and a centralised model where a single ICT support service manages systems end to end. This model has resulted in:

- Fragmented responsibilities for application support and management that are not clear;
- 53% of systems include a key person dependency risk due to support being managed by one subject matter expert off the side of their desk;
- multiple fragmented management tools including spreadsheets, Access databases and multiple partial-knowledge bases;
- inability to see an overall view of application support health and management statistics; and

[4] There is a solution architecture capability which is applied on a project by project basis to design solutions, but no overarching planning and governance is in place.

- a complex support service model, as depicted in the following diagram.



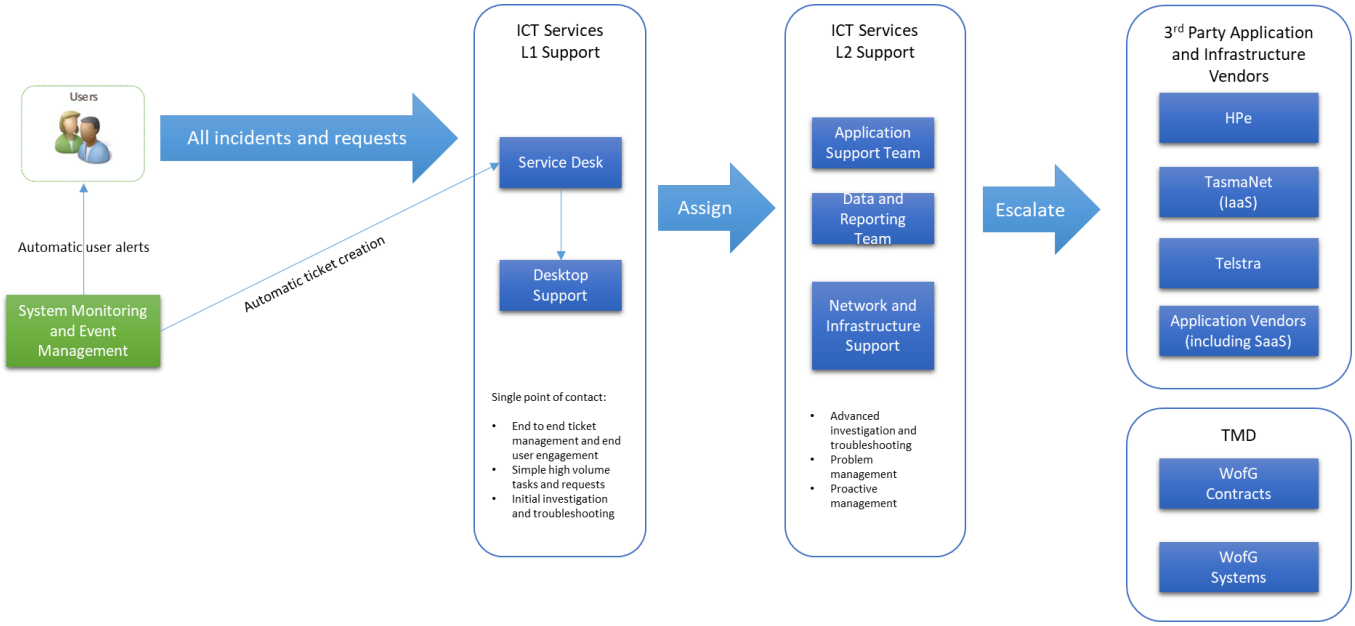
9.2 Target State

The desired target state is to have a more centralised support where possible, with appropriate staffing levels, skilled resources, and fit for purpose management tools. The support model is underpinned by business control mechanisms to ensure the model provides control and better outcomes to Agency outputs:

- Defined and agreed service levels for support and availability based on system criticality and risk appetite.
- Assigned business system ownership and support RACI, which includes business owners, functional stakeholders and subject matter experts.
- Appropriate budgetary measures, including within project business cases to ensure adequate support resource levels are funded.
- An uplift in ICT support skills and capability.
- A single point of call for all systems and all users (the service desk).
- Uplift capability through support tools:

- service desk;
- knowledge base;
- CMDB (Configuration Management Database);
- reporting;
- secure password repository; and
- monitoring and event management

The target model is depicted in the diagram below:



9.2.1 Benefits

The benefits of the target state extend to individual outputs and the Agency as a whole, and are as follows:

- remove key person dependency risks;
- consistent support approach and processes;
- one point of call for all systems and users;
- free up business resources to concentrate on their core business;
- achieve economies of scale with a shared pool of IT support resources (people and technology);

- improve knowledge management and support/system health metrics through centralised monitoring and reporting;
- enable proactive problem management; and

It is acknowledged that some outputs require immediate on-site support for their systems (e.g. the courts cannot sustain an outage of the recording system and require immediate rectification). It is proposed that an on-site support resource is deployed on a rotating basis to ensure knowledge sharing and reduce key person dependencies.

9.3 Transition approach and change management

It is acknowledged that there are both positive and negative implications of this change, and some individual outputs may perceive this as a *decrease* in service capability. The following negative impacts have been identified and need to be managed as part of the change implementation plan:

- Financial. It is acknowledged that this change will not reduce costs short term as in most cases the business-embedded support resource will be retained by the output in addition to the additional support allocation within ICT. While this can be perceived as driving up total cost for the Agency, the following counterfactuals are considered to outweigh the increase in cost:
    - Business-embedded resources are freed up to perform a greater level of output for their core business function.
    - Dedicated embedded support resources may be able to transfer into the centralised ICT support and expand their skills and system coverage.
    - Long-term reduced costs as key person dependency risks are not realised.
    - Long term reduced costs from improved system support capacity resulting in improved system health.
- Political (internal). It is acknowledged that moving to a centralised model will mean relinquishing full control of support for some outputs. However, the system ownership model, service level agreements and governance mechanisms will ensure that business system owners retain control of the direction and support levels for their systems. The improved and consistent service quality should also outweigh this by providing better reporting and access to increased capabilities and services. Business outputs are freed up to concentrate on core business activities.

- Resources and capabilities. The current ICT support team is capacity constrained and also requires a capability uplift before a centralised ICT model can deliver improved business outcomes. In addition, any changes to resource allocations, roles and reporting lines needs to be carefully managed in accordance with HR policies. This is to ensure appropriate consultation, change management, training and support is provided for individual resources and managers.

As such, the transition needs to be managed as a project to ensure all desired outcomes are achieved and that the transition is well communicated, smooth and beneficial for all stakeholders. Such a change needs to be seen as a 'journey' and will take up to 3 years to complete, and will be incrementally delivered as part of the change scope for funded ICT projects.

10 PORTFOLIO MANAGEMENT AND PROJECT DELIVERY

The Project Management Office have, in the past, worked somewhat in isolation from the ICT Group to deliver to business requirements without an appropriate level of ICT engagement or involvement.

Projects are typically submitted by outputs as needed, and are not considered in a more strategic or portfolio manner. This has led to the siloed solution approach and lack of prioritisation and overall architectural oversight in relation to the benefits and outcomes of the initiative.

The current engagement model has resulted in poor project budgeting from a technical labour perspective and lack of involvement and engagement in the future operational support requirements. Forward planning can result in more effective resource utilisation across projects in the program of work, reducing recruitment and on boarding effort, and increasing momentum.

Program level governance and visibility has been lacking or ad-hoc, with inadequate portfolio reporting and monitoring. The governance model described above in *Section 7 - ICT Governance* will remediate this.

Within projects the project management methodology is immature and inconsistently understood and applied. Work is required to train and embed a consistent methodology to ensure consistency and to facilitate a more scalable project resource pool.

The project resource pool itself is not optimal. For example, there are unrealistic expectations on Business Analysts to perform multiple additional roles such as Project Manager, Test Manager and Change Manager. This leads to sub-optimal outcomes due to lack of skillset and capacity.

A portfolio planning approach with effective governance and business cases will allow for the right mix of resources to ensure projects succeed.

11 APPLICATIONS STRATEGY

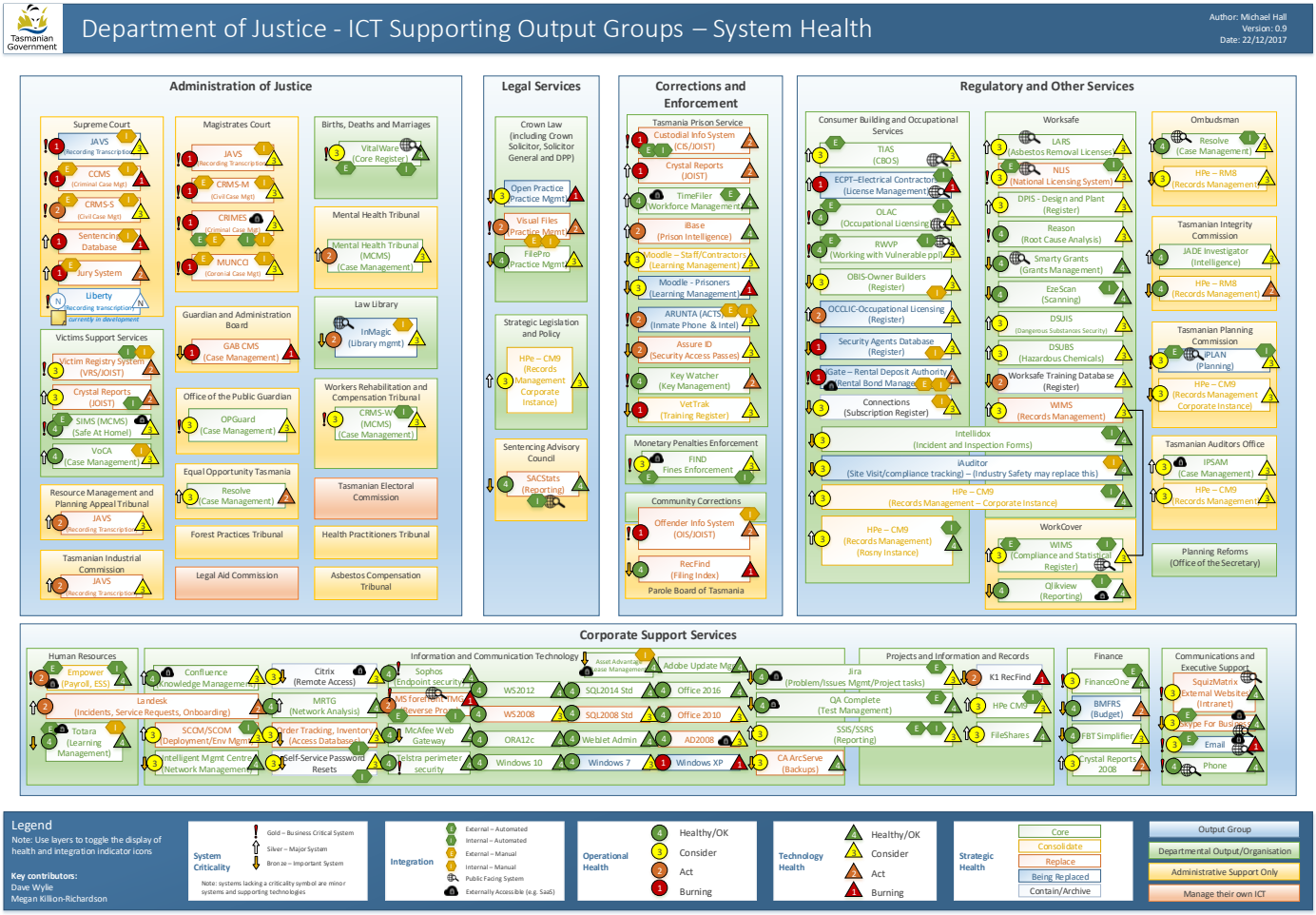
11.1 Current State

Application Health has not been tracked within the Department, which has resulted in a short-term view being taken and a lack of risk, issue and opportunity information to influence or inform decisions and forward planning. A common pattern is that systems are implemented on a limited budget and compromise is made on which requirements are cut from scope. However, there is no ongoing plan, budget or resource capacity to improve the system after initial go live, and no scope to implement additional features and issue rectification. Over time, the health degrades and a new system is purchased rather than improving the existing system, which is seen as having accumulated too much technical debt.

The bottom up system health assessment has identified:

- business criticality of current systems (how important is this system to the success of the business);
- operational health and age of current systems (how efficient, effective and trusted is the system to meet business needs);
- technology health of current systems (how available, supportable and secure is the system); and
- strategic health of current systems (is this the right system for us)

The results are summarised in the diagram below:



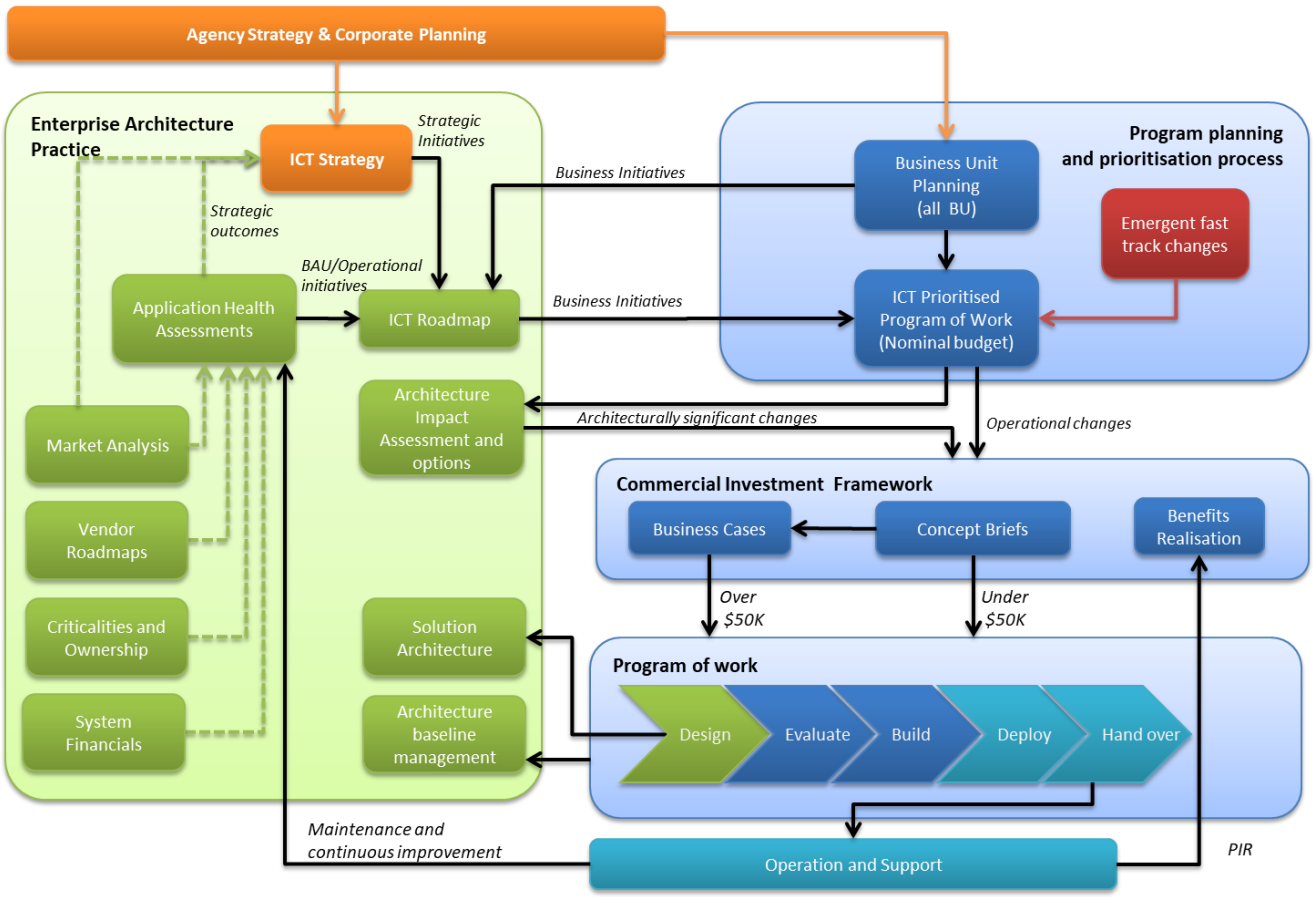
A number of systems can be seen as requiring urgent attention to either upgrade, replace or consolidate, and some systems carry significant risk. In their current state, many of the systems are unable to enable the realisation of the ICT vision or objectives. A remediation plan has been developed with initiatives and prioritisation factors. This is described below in *Section 12 ICT Roadmap*.

11.2 Management Approach

A holistic application lifecycle management approach is required to break this cycle and support:

- ease of administration;
- reduced long-term costs;
- continuous improvement; and
- continuous re-alignment to business needs.

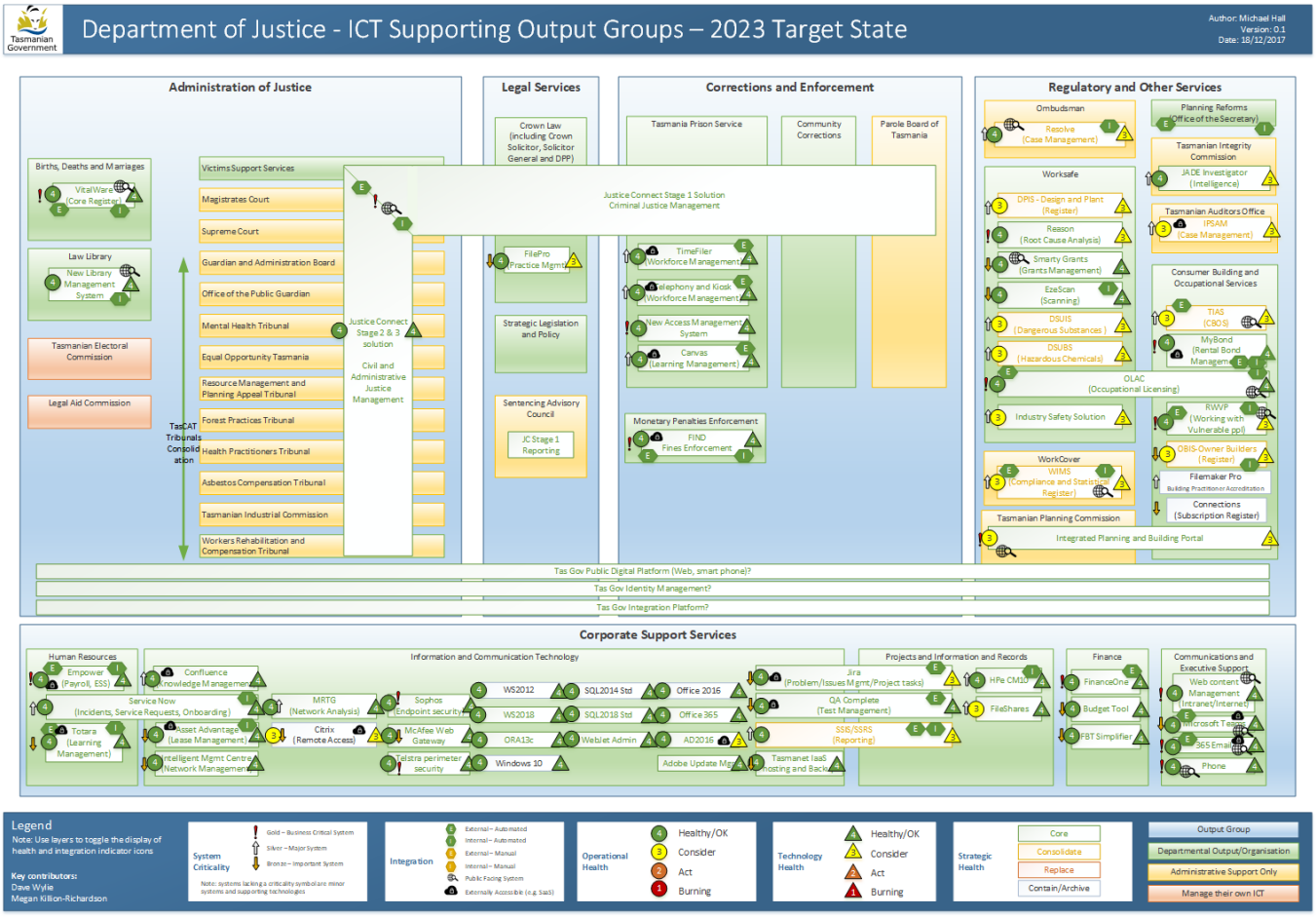
An ongoing integrated approach involving strategic planning, program management, and continuous improvement through support and feedback is required, as illustrated in the diagram below:



Work will need to continue to analyse and assess applications utilised, to ensure that the most effective and efficient, functionally robust applications are utilised within the organisation.

11.3 Target State

As a result, the target state for applications within the department sees a large scale rationalisation and replacement program resulting in far fewer systems, as depicted in the diagram below:



More detail is provided below on an output-by-output basis:

11.4 Administration of Justice

Within the administration of justice are a number of distinct outputs, each with their own strategy and ICT requirements:

11.4.1 The Courts and Law Library

The courts are currently using a range of disparate, aged systems including Access databases. These systems have very limited integration with each other and also externally to Tasmania Police and downstream functions such as Prisons, Community Corrections and Victims Support. There is also a heavy reliance on manual paper based processes. This has resulted in a number of serious issues that have received media and Government attention, and triggered multiple external reviews.

The internal system health review also reaches the same conclusions that these systems are a burning platform and carry significant operational and strategic risk, and therefore a holistic response is required.

The Justice Connect Project has commenced with an intent to transform the end to end processes and data flows between Police, DPP, the courts, Prisons and Community Corrections. It will also support better information sharing to downstream functions such as Victims Support Service, Safe at Home, DHHS and federal agencies. The key objectives of this project are:

1. digitise;
2. streamline;
3. share; and
4. improve data quality and timeliness.

The project aligns to the overall strategic objectives and principles within this strategy and will be a critical initiative that will underpin and become the cornerstone of this Strategy.

11.4.2 The Tribunals

Tribunals Rationalisation will result in the amalgamation of a number of tribunals into a single unit with shared underpinning technology enabling common toolsets, processes and capabilities. At this stage the project remains unfunded, and is subject to approval by Cabinet as part of a formal business case budget submission.

11.4.3 Births, Deaths and Marriages

The Vitalware register is expected to be maintained, with processes improved through the implementation of an online portal for registering births, deaths and marriages and facilitating the national document verification service.

11.4.4 Guardianship

The Guardian Administration Board will benefit from a case management system replacement, and is likely to be considered in the case management rationalisation project. The Office of the Public Guardian will also be considered in this same project, though may simply require some improvements to their existing case management system OPGuard.

11.4.5 Tasmanian Industrial Commission

The need for a case management solution has been identified and should be considered as part of the case management rationalisation project.

11.4.6 Legal Aid Commission

The Legal Aid Commission does not currently receive ICT support from the Agency. Initial work may be required to assess whether they would benefit from utilising shared services.

11.4.7 Common initiatives

In addition to output specific initiatives, benefits are expected from the following:

- Document Management expansion and consolidation
- Website tender and uplift with support for e-forms and dashboards
- Video conferencing
- Case management system rationalisation

11.5 Legal Services

The legal services output group has identified a number of shortcomings in the practice management system Visual Files, and its vendor. An assessment for a suitable replacement that is integrated with Police and the Courts will form part of the Justice Connect project. A repository for Deeds and Opinions has also been identified by Crown Law. In addition, the following initiatives will benefit this output group:

- Document Management expansion and consolidation
- Website tender and uplift with support for e-forms and dashboards
- Analytics and reporting
- Video conferencing
- Case management system rationalisation

11.6 Corrections, Enforcement and Consumer Protection

This output group is diverse and is impacted by a number of planned and in-flight initiatives which are outlined below.

11.6.1 Tasmania Prison Service

Justice Connect will replace the existing Custodial Information System (JOIST) with a new system integrated to the courts and downstream functions, and supporting the prison intelligence capability. Improvements to training platforms and a replacement of the prisoner telephony system

are also planned. In addition, consideration is being given to digital customer self-service through use of prison kiosks.

11.6.2 Community Corrections

Community corrections will be impacted by Justice Connect with the replacement of the Offender Information System (JOIST) with a new system integrated to the courts and downstream functions, as well as the Parole Board. This will result in improved case management and reporting, and better quality data and information sharing.

11.6.3 Parole Board

The Parole Board will be impacted by Justice Connect and will gain relevant access to the JOIST replacement and new case management capabilities.

11.6.4 Monetary Penalties Enforcement Service

The fines management system, FIND, is fundamentally sound with regards to its system architecture, and needs to be maintained and improved, with the following key initiatives planned:

- System upgrade to version 4.6 to be completed by March 2018 to enable future work.
- System upgrade to version 5 to be completed by July 2018.
- Mandatory tender for Infrastructure hosting, system and database administration, and migration away from TMD to a Tasmanian cloud provider by December 2018, since TMD is moving away from support.
- Mandatory tender for application development and support contract, since CGI contract expires March 2019 and cannot be extended.
- System upgrade to version 6.
- Integration impacts from the Justice Connect solution, and Tasmania Police's *Project Unify* (which will include regression testing at minimum).
- Continuous improvement program of work.

This constitutes a significant program of work for FIND, which is currently under-resourced, as indicated in the *2016 Quill Australia Report on the FIND Governance Model*. This strategy reiterates the need to invest in more resources to support the program of work described above, since the current team is key person dependent and unable to respond quickly to requested changes.[5] The

[5] As an example, it is common for business specifications for major releases to have been signed off 3 years prior to release go live. Such three-year turnaround times are increasingly unacceptable in a rapidly changing environment.

team in its current form is unlikely to be able to meet the required changes in the given deadlines, and the burden placed on key resources is unsustainable.

Further consideration should be given to whether FIND could appropriately be managed by a centralised team with more knowledge sharing, or whether a dedicated team would provide the best outcome. Additional changes to the governance and ownership are also required to ensure increased sense of stakeholder ownership and strategic planning. It is noted that FIND is jointly 'owned' by MPES and Tasmania Police Service, however funding is currently entirely from MPES.

11.6.5 Consumer Building and Occupational Services

CBOS has a number of systems that manage licenses and accreditations of various kinds. Key projects include:

- Further OLAC (Occupational Licencing Audit and Compliance system) phases to replace and consolidate existing legacy systems with a single licence management platform with online customer registration and access.
- Further stages to the Registration for Working With Vulnerable People system (RWVP) to enable online payments, re-applications and phot capture, business reporting, and an employer portal.
- The MyBond project will replace the current iGate rental deposit management system and allow greater flexibility to support online customer interactions and reporting.

11.7 Regulatory and Other Services

There are a number of separate outputs within this group:

11.7.1 Worksafe

Worksafe aspires to undertake an output-wide digital transformation, reviewing all processes to digitise, automate and streamline. This will be a major undertaking that will position Worksafe to align with modern expectations and achieve higher quality outcomes and efficiency. It may be worth considering whether an agency team could begin a digital transformation process with Worksafe, and then move onto other outputs, bringing the intellectual property and experience gained to improve the transformation efforts across the agency.

An example of this at a smaller level is the Industry Safety project, which will assist inspectors and auditors to have access to digital tools, streamlined process and better information sharing and analysis.

11.7.2 WorkCover

WorkCover will be impacted by the activities of Worksafe with regards to the replacement of the shared WIMS system. It is envisaged that while Worksafe will cease using WIMS for workplace attendance records, WorkCover will continue to use it as a register of insurance compliance to meet the requirements of the Workers Rehabilitation and Compensation Act 1988. Therefore this system will need to be maintained.

11.7.3 Ombudsman

The case management system Resolve will be reviewed as part of the case management rationalisation project, and the current records management system HP RM8 will likely need to be upgraded and consolidated to the single HP CM9 platform as part of the records management consolidation project.

11.7.4 Tasmanian Integrity Commission

The intelligence system Jade Investigator will continue to be maintained, while the current records management system HP RM8 will likely need to be upgraded and consolidated to the single HP CM9 platform as part of the records management consolidation project, with appropriate security and access protocols as required for the commission. It is noted that a separate instance of CM9 may be required.

11.7.5 Tasmanian Planning Commission

The current planning system, iPlan, has vendor support risks and is due for replacement as part of a major initiative for a state-wide integrated planning platform, in line with federal initiatives such as the Red Tape Reduction Program.

11.7.6 Tasmanian Auditors Office

The Lotus Notes cloud based audit management system IPSAM is likely to remain in use in the near future, and the dedicated records management instance of CM9 will be reviewed as part of the records management consolidation project, but may need to remain as a separate instance.

11.8 Underpinning Application Strategy

In addition to output specific items, there are a number of Agency-wide application objectives, which are outlined below.

11.8.1 Integration capability

In view of the push towards greater digitisation of business processes, the need for information to be shared between outputs and systems will require that strategic integration capability is used.

This is in order to avoid a proliferation of point-to-point interfaces that will in time become an administrative burden. A modern integration capability such as an enterprise service bus, or micro-services platform may assist the Agency to manage consistent integration capabilities, and create efficiencies through re-use and common interface models and methods. It is envisaged that this capability will be introduced to the Agency as part of the Justice Connect project, but implemented in such a way as to be extensible for other use cases.

The integration capability also needs to be underpinned by strong data governance and a good understanding of data models.

11.8.2 Data Warehousing and Analytics

Access to good information is a key requirement of any modern business. While the Agency has made good progress on operational reporting through the use of Microsoft Reporting Services, there are only two people in the organisation supporting this. These are not dedicated reporting resources and they are already operating at capacity, which is impacting the ability for outputs to request new reports and changes to reports. It has also led to a lack of documentation around reports.

Investment is required to uplift the capacity and capability in the reporting and analytics space. This is especially pertinent as new systems and processes are introduced which will have new reporting and dash-boarding requirements, and data models. The reporting capability will require:

- a data warehouse:
    - this will be supported by the integration capability described above;
- continued use of Microsoft Reporting Services for operational reports;
- the implementation of an analytics and dash-boarding system;
- new processes for requesting and defining reports;
- a metadata repository tracking data dictionaries and data lineage; and
- additional capacity and expertise in the areas of data analysis, business analysis, data warehouse and report development.

Quality of data is vital for the effective management of each function within the organisation. The complexity of integration and data flows along with the reliance on data to enable effective servicing for the customer compounds this further. Business data stewards need to be appointed and hold accountability for ensuring internal data quality and integrity in source systems. This function can be supported by data exception reports, but ownership of data quality must remain within the business outputs.

Regular data reconciliation and maintenance will ensure that the information utilised and future reporting and analytics are of the highest quality to achieve the objectives required. The ability to be able to rely on the data will be critical to the decisions that will need to be made over the period and will be especially relevant in a competitive market.

The ability to utilise the data to gain insight into the customer and to have effective targeted campaigns will also be fundamental.

11.8.3 Solutions as a Service

Cloud services are becoming firmly established as the mainstream delivery model for ICT worldwide. Following on from the whole of Government direction to utilise Infrastructure as a Service, the Agency will adopt an 'as a Service' philosophy, which could comprise of Infrastructure (IaaS), Platform (PaaS) or Software (SaaS) as applicable, based on the following principles:

- Utilisation of these services are optimal for businesses where on demand infrastructure is required to handle peak loads or where outright capital purchasing of physical infrastructure, including ongoing lifecycle replacement, is not cost effective.
- Software as a service does not lend itself to customisation. Therefore, it is best suited to commodity systems that do not need to be adapted to specific business needs, or where the business can adapt its processes to meet the system functionality.
- Well-functioning Software as a Service may not always be hosted on shore in Australia, and so data sensitive applications may not be suited to SaaS, in which case software that can be hosted on a local IaaS or PaaS offering may be a better option.
- The availability, security, capacity and service requirements of the system will be taken into account when selecting these services.

11.8.4 In-house Developed Applications

There are a number of in-house developed applications still in use within the Agency. There is also a reliance on over 4,000 Access databases. These can be difficult to maintain and manage, creating key person dependency risks and resource bottlenecks. As such, they can hold back innovation and agility.

This IT strategy recommends avoiding in-house developed applications and seeking to replace existing systems with supported off the shelf solutions where possible. It is understood that it will take a considerable amount of time and effort to transition from the current state to meet this aspiration.

11.8.5 Information Management

The information management function has historically been separated from the records management function in the Agency, with the former residing in the project management office. This Strategy recommends merging Records and Information Management under the current Records team in order to:

- Consolidate and strengthen the records and information management capability and capacity;
- Ensure ongoing rollout of the Information Management Framework;
- Continue to develop and manage the Information Asset Register; and
- Focus the Project Management Office on project delivery and program management.

11.8.6 Infrastructure and End User compute

The current migration from on premise server infrastructure to Infrastructure as a Service (IaaS) has delivered the following benefits:

- Significantly sped up server provisioning;
- Provided a foundation for future flexibility as we rationalise applications;
- Increased system reliability through modern, supported technology;
- Reduced management overhead and effort;
- Reduced system outage risk through higher availability SLAs and capabilities; and
- Aligned to State Government directives to outsource to infrastructure as a service.

While the initial migration to IaaS is still under way, further work is required to maximise the benefit of the new platform, and this includes:

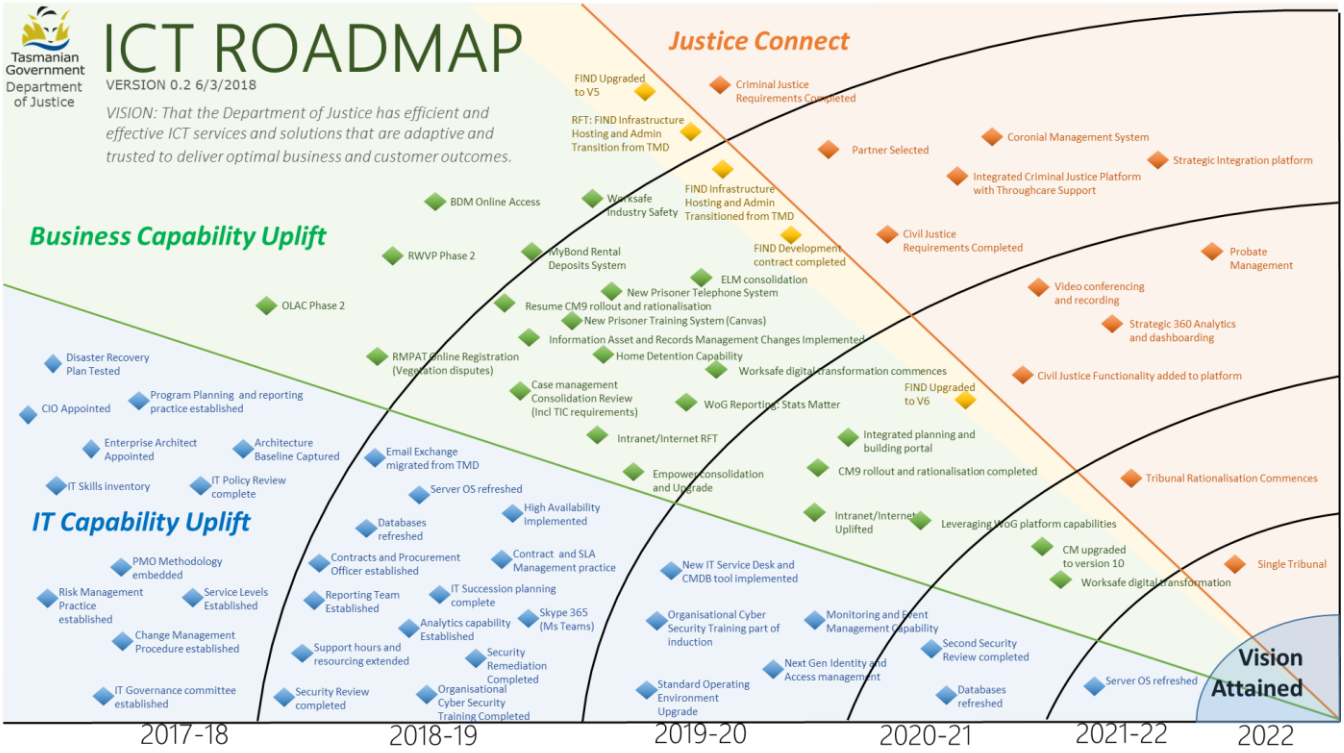
- Introducing capacity management;
- Reviewing the existing deployment and capacity and optimising;
- Independent review of SQL Server database architecture and optimisation for performance and best practices;
- Creation of a disaster recovery plan, and underlying mechanisms, which may include:
    - Agreeing with business owners:

        - RTO - restore time objectives (the time that can be taken to bring a system back online)
        - RPO - restore point objectives (the point in time data can be restored to after a system failure that may include data loss)
        - RLO - restore level objectives (the level to which a system must be restored (e.g. can it run at half capacity temporarily))
    - Implementing high availability for business-critical systems;
    - Implementing required changes to meet the agreed RTO, RPO and RLO;
    - Changes to log shipping for transactional databases; and
    - Developing and testing a disaster recovery plan annually.

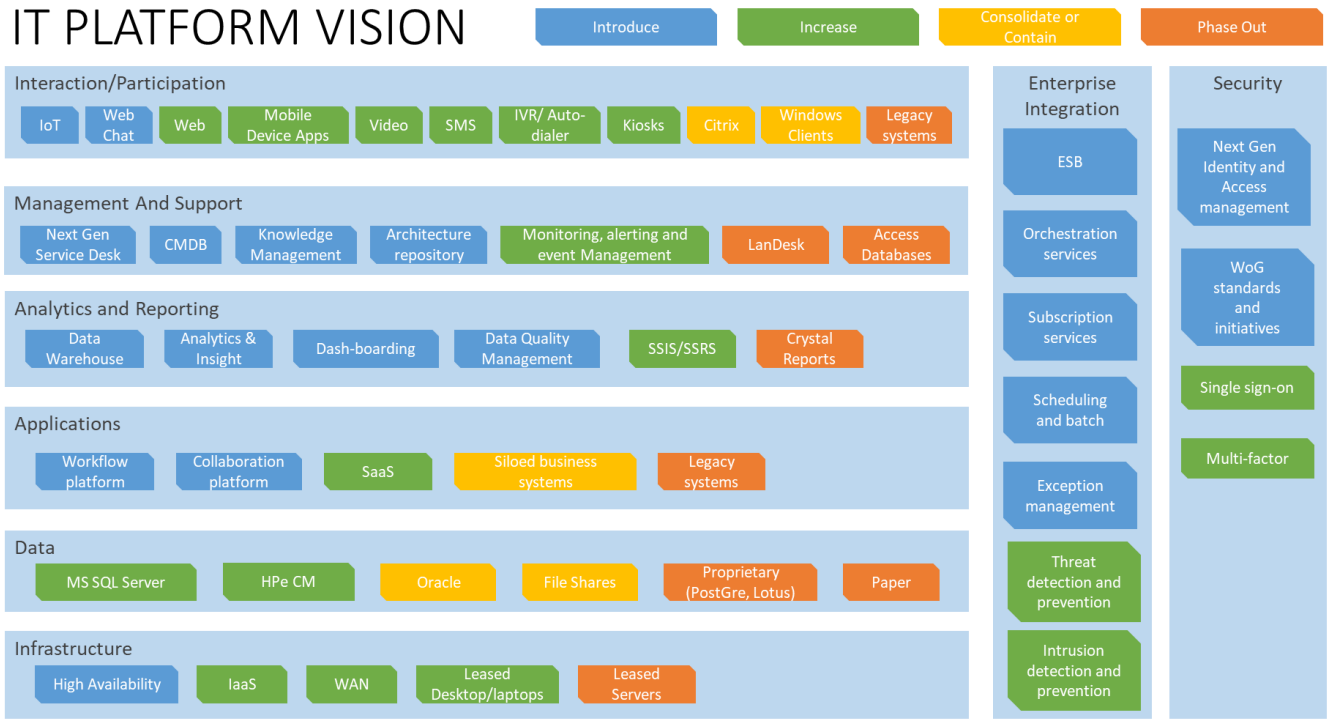
Continuing to lease desktops and peripherals will allow the agility that will be required to keep up with the fast-paced changes in technology, whilst avoiding stranded assets.

12 ICT ROADMAP

The key initiatives to achieve this vision are set out in the IT Roadmap, noting that some of the initiatives are already funded and others will require funding submissions.


Tasmanian Government
Department of Justice
ICT ROADMAP
VERSION 0.2 6/3/2018
VISION: That the Department of Justice has efficient and effective ICT services and solutions that are adaptive and trusted to deliver optimal business and customer outcomes.
Justice Connect
Business Capability Uplift
IT Capability Uplift
FIND Upgraded to V5
Criminal Justice Requirements Completed
RFT: FIND Infrastructure Hosting and Admin Transition from TMD
Partner Selected
Coronial Management System
Strategic Integration platform
Integrated Criminal Justice Platform with Throughcare Support
FIND Infrastructure Hosting and Admin Transitioned from TMD
BDM Online Access
Worksafe Industry Safety
Civil Justice Requirements Completed
Probate Management
FIND Development contract completed
RWVP Phase 2
MyBond Rental Deposits System
ELM consolidation
Video conferencing and recording
New Prisoner Telephone System
OLAC Phase 2
Resume CM9 rollout and rationalisation
Strategic 360 Analytics and dashboarding
New Prisoner Training System (Canvas)
Information Asset and Records Management Changes Implemented
Disaster Recovery Plan Tested
RMPAT Online Registration (Vegetation disputes)
Home Detention Capability
Worksafe digital transformation commences
Civil Justice Functionality added to platform
Case management Consolidation Review (Incl TIC requirements)
FIND Upgraded to V6
CIO Appointed
Program Planning and reporting practice established
WoG Reporting: Stats Matter
Intranet/Internet RFT
Integrated planning and building portal
Enterprise Architect Appointed
Architecture Baseline Captured
Email Exchange migrated from TMD
Empower consolidation and Upgrade
CM9 rollout and rationalisation completed
Tribunal Rationalisation Commences
IT Skills inventory
IT Policy Review complete
Server OS refreshed
Intranet/Internet Uplifted
Leveraging WoG platform capabilities
High Availability Implemented
Databases refreshed
CM upgraded to version 10
Single Tribunal
PMO Methodology embedded
Contracts and Procurement Officer established
Contract and SLA Management practice
New IT Service Desk and CMDB tool implemented
Worksafe digital transformation
Risk Management Practice established
Service Levels Established
Reporting Team Established
IT Succession planning complete
Skype 365 (Ms Teams)
Organisational Cyber Security Training part of induction
Monitoring and Event Management Capability
Analytics capability Established
Change Management Procedure established
Support hours and resourcing extended
Security Remediation Completed
Second Security Review completed
Next Gen Identity and Access management
Vision Attained
IT Governance committee established
Security Review completed
Organisational Cyber Security Training Completed
Standard Operating Environment Upgrade
Databases refreshed
Server OS refreshed
2017-18
2018-19
2019-20
2020-21
2021-22
2022

This vision is to be achieved through investment in new strategic platforms, leveraging commodity products and strategic outsourcing partners, and implementing new IT capabilities to fill current capability gaps. The envisaged platform is summarised in the diagram below:



13 RISK MANAGEMENT

13.1 Risk based decision making

Investment priority and Service levels will be based on the risk profile and risk appetite, which aligns to the business criticality of the system or service.

Risk management in general has been lacking, and a discipline of formal risk management within ICT needs to be established and owned. It is acknowledged that the current corporate risk management framework can be too strategically focussed to be relevant for many ICT and project risks, and so three risk classifications and frameworks are proposed:

1. Strategic risks follow the corporate risk management framework.
2. Operational risks follow the ICT risk management framework (to be developed).
3. Project implementation risks follow the project risk management framework (to be developed).

13.2 Risk Appetite

The risk appetite for individual systems is based on a standardised system criticality profile:

Criticality 1 – Gold

Gold systems are systems that require high availability, since outages seriously affect operations and lead to high financial, safety or reputational risk. A maximum tolerable outage for a gold system would be 3 hours as a general rule. Gold systems may include payroll, public facing websites, key revenue generating and safety systems.

Criticality 2 – Silver

Silver systems are used frequently or extensively, and outages would cause difficulty but manual work-arounds could be sustained for up to 24 hours if required.

Criticality 3 – Bronze

Bronze systems are used by isolated groups, and outages can be tolerated for up to 72 hours with manual work-arounds.

13.2.1 Criticality Based risk Management

Providing availability server levels that can actually be met comes at a cost. In order to facilitate appropriate response to risk appetite for business criticality, the following underlying support and availability mechanisms need to be in place:

		Business System Criticality		
	Key	1-Gold	2-Silver	3-Bronze
Hardware	1. Must be under warranty 2. Extend warranty (once only) 3. Extend warranty (twice only) 4. Operate at risk	2	3	3
Software	1. Must be supported version 2. Unsupported version OK	1	1	2
Vendor Support	1. 24/7 support required 2. B/H support only 3. Best effort 4. None	1	2	3
Internal support	1. 24/7 support required 2. B/H support only 3. Best effort 4. None	1* Case by case-on call	2* Case by case heightened support times	2
Disaster Recovery	1. Hot Failover (instant RTO) 2. Cold failover (20-60 mins RTO) 3. Backup – dedicated server (8 hours – 5 days RTO) 4. Best effort	2	3	3
Backups	1. Backed up 2. Not backed up	1	1	1

13.3 Key Risks

The following have been identified as key risks to this Strategy, and will require mitigation and review by the ICT Governance Committee:

1. There is currently no CIO to own and drive the implementation of this strategy and ensure adequate stakeholder engagement.
2. Lack of top-level support undermines the initiatives, progress and priority of the strategy.
3. Lack of stakeholder buy-in from independent outputs and statutory bodies becomes a blocker to strategy implementation.
4. Resistance to change, and inadequate change management.
5. Competing priorities between outputs.
6. Pre-requisites and interdependencies between projects impede ability to schedule delivery of strategic objectives.
7. There is insufficient staff capacity and training to effect the changes.
8. Inability to uplift the ICT capability leads outputs to lose confidence in a centralised delivery model.
9. Insufficient budget allocation to implement the strategy.
10. Election cycle impacts funding, priorities and organisational structure.
11. The funding model and approach does not support successful investment and cost recovery.
12. The age, health and current support levels for systems prevents innovation and holds back progress.
13. The disaster recovery capability is inadequate.
14. New high criticality directives, requirements or incidents cause a change in direction or impede progress.

14 KEY ASSUMPTIONS

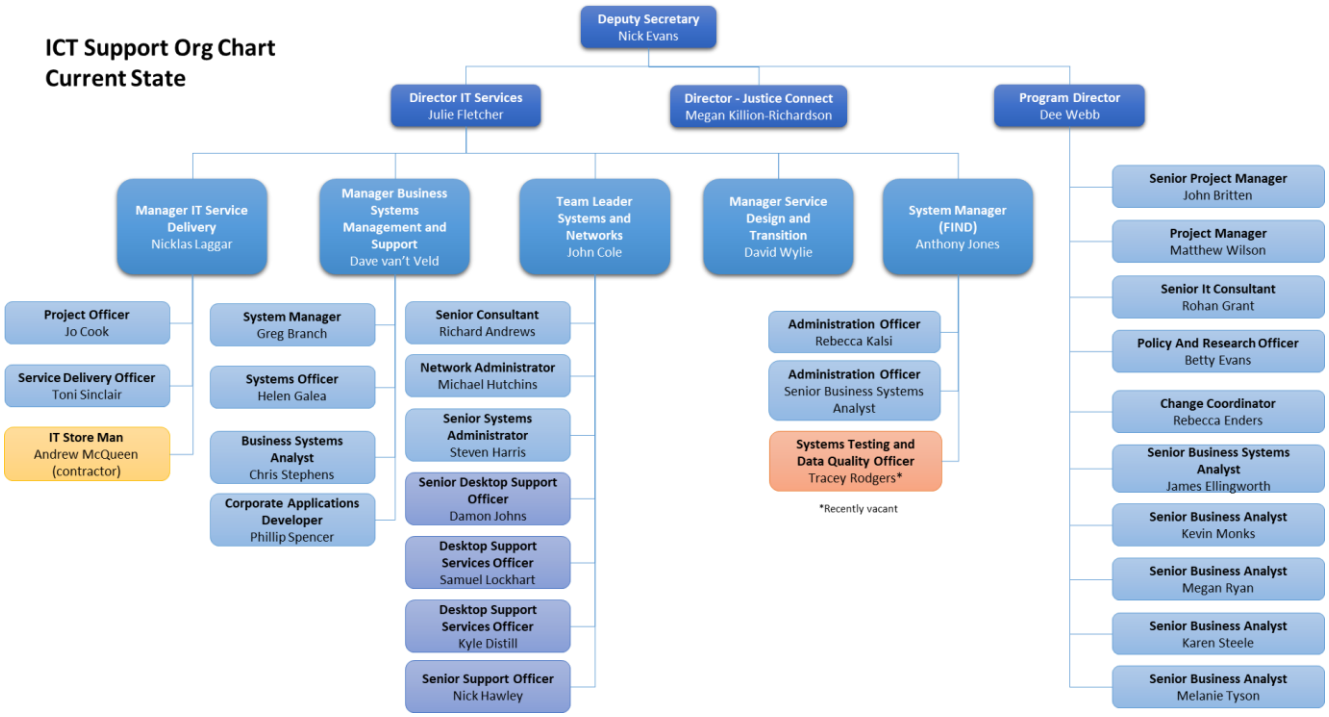
The following assumptions have underpinned this strategy:

1. Top level support is provided to effect the required cultural change amongst the full range of outputs and independent statutory authorities.
2. A CIO will be appointed to drive the strategy implementation.
3. Funding can be secured to implement the strategy.
4. There is an appetite and cultural imperative to continuously improve and challenge the status quo.

15 PEOPLE

The current organisational structure contains 35 staff, including eight managers, with some staff serving part time and on fixed term contracts. There are also numbers in the dozens of embedded system administrators throughout the agency, which have not been included in the counting.

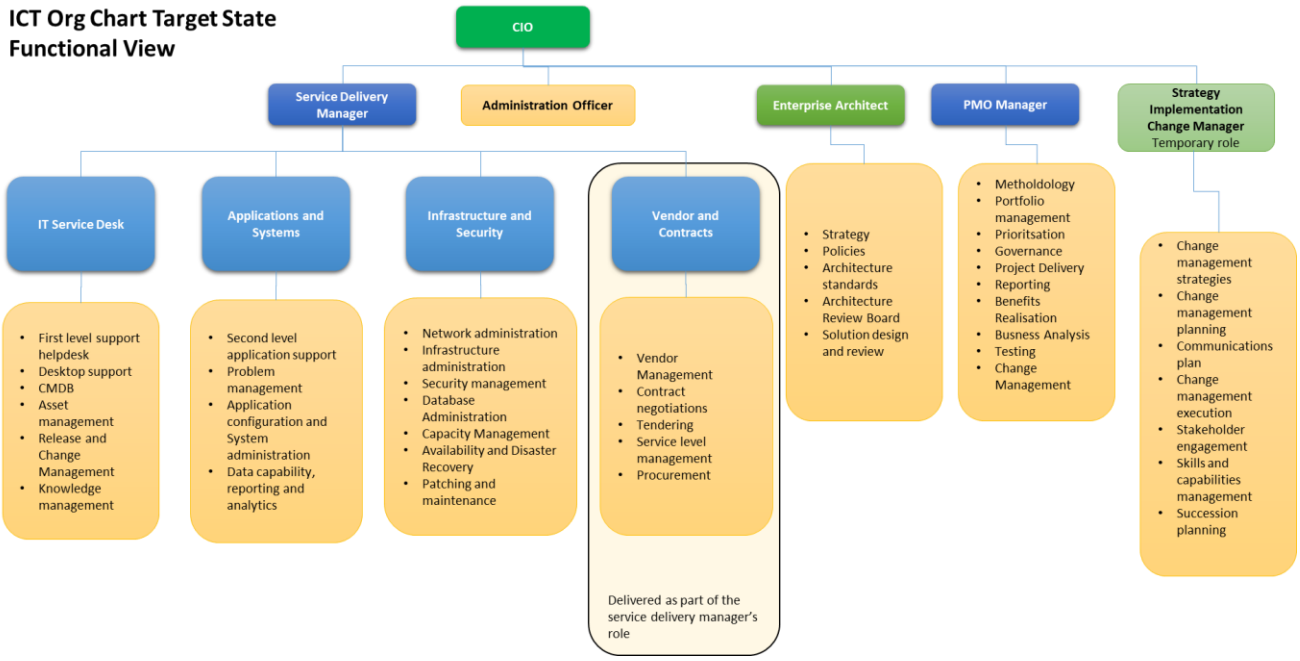
The structure itself is depicted below:



The above model is not best practice, but rather bears the marks of organic evolution. It contains roles of the same or similar nature duplicated in vertical streams, and vertical streams themselves containing duplication of function. In addition, there are a number of role gaps, and some employees complain of lacking role clarity.

The ICT Capability and Maturity model from Section 2.3 highlights the areas where there is currently either deficiency in capability or resourcing. In summary, the current structure of the ICT unit has been constructed to deliver the minimal requirements for operating a business as usual operational environment, thus resulting in a reactive 'firefighting' team.

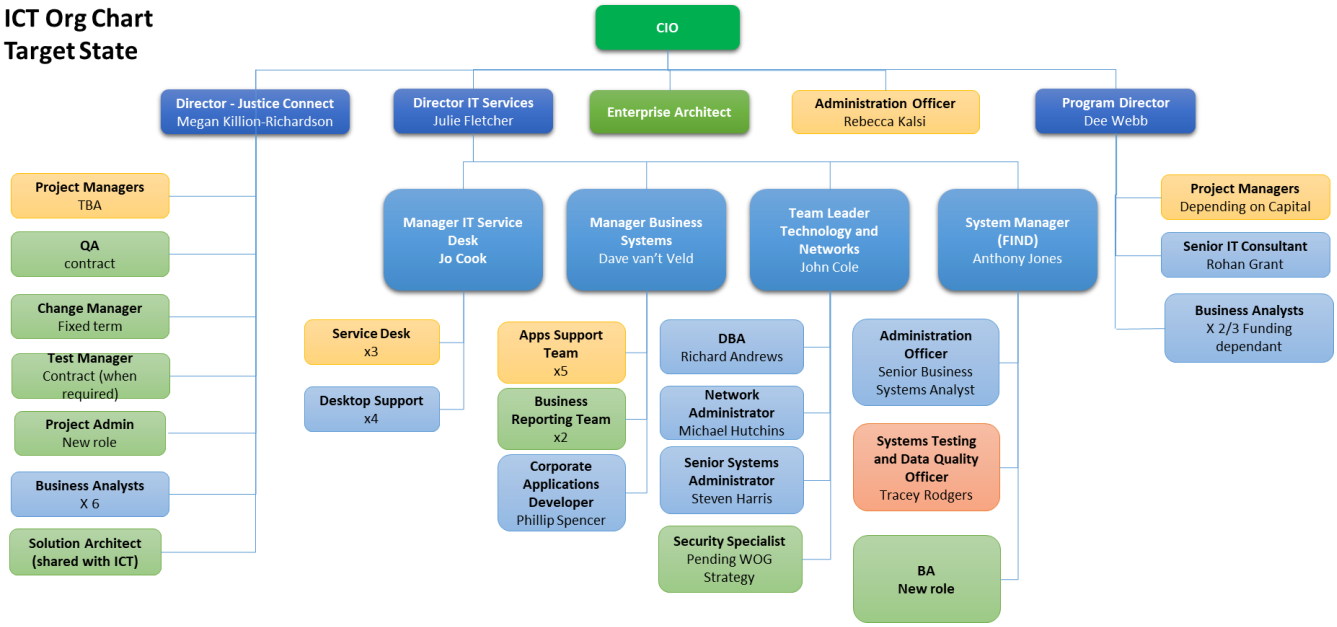
Below is the proposed functional target state:



Resource and workforce management, planning and procurement will be fundamental, within the delivery teams and the wider organisation from a change, impact and implementation perspective. Highly skilled and experienced resources will be required to deliver the strategic initiatives, most probably, short term hire to deliver agreed portfolio and transformation over the period.

It is anticipated that resources required to deliver projects will funded by the specific project or program which may require Treasury SIIRP business case approval and funding.

Succession planning, along with the intent of reducing reliance of key subject matter experts will also be vital to delivering outcomes required. A culture of continual cross and upskilling, along with commitment to documenting system support procedures will be critical to reducing key person dependencies over time. Aligned with ensuring contemporary ICT skills and capabilities are relevant as technology and systems evolve will need to closely assessed, monitored and addressed if required. This may mean a higher level of investment in Training and Development across the Agency.



16 FINANCIAL

The ICT spend of $7.6m per annum currently equates to 5.30% of the Agency annual operating budget. The majority of this spend is for internal labour costs, operational systems support along with leasing or subscription payments for infrastructure. There is limited capital investment in new technologies or transforming business processes and functionality. This lack of investment, along with a siloed approach to solution design and support has placed the Agency in a situation where costs will continue to escalate unless a longer term and centralised approach is adopted.

According to the Australian Government ICT Trends Report of 2015-2016 the average spend by department was 10.4%. Trend towards operating cost model is increasing as leasing and 'As a Service' models continue to be adopted.

Whilst there will be an expected reduction in wasted and non-productive effort through process automation and alignment of systems to business process improvements, no overall net cost reduction is expected from this Strategy, as it is primarily a remedial strategy based on the current system health and risk profile.

16.1 Operational labour costs

Current resource allocation is insufficient to enable an increased maturity level required for a sustainable, well performing department. To elevate from the current operational "reactive" mode to a 'proactive' approach it is anticipated that labour costs would need to increase by a minimum of $435K* per annum.

Current ICT Establishment costs at initial view, looks like $1.669m per annum spend, when in reality it is $2.126m (funded by trust fund allocations).

A conservative total for the minimum required would be $2.561m.

16.2 Ongoing Asset Lifecycle Investment

Once invested in an asset, be system or infrastructure, there is a generally a requirement for ongoing continual investment in order to maintain the asset to a contemporary and functional standard. It is estimated that this would be an ongoing commitment of between $1.5m - $2m per year in Major upgrades or system support.

16.3 Strategic Initiatives

Separate to JC an estimate of $4-$5m capital spend would be required over the three year period to get to a stable state.

16.4 Future Spend Required

Considering the estimated increase labour costs (to a minimal level), along with ongoing funding required to maintain systems and platforms, current spend would elevate from 5.30% to 6.74% per annum of total operating expenditure, still considerably less than the national average in 2016 of 10.4%.

Full assessment of current vendor/system support and maintenance costs has not been completed and will form part of the strategic initiative regarding vendor and contract management, and also will be continuously revisited as part of the ICT Governance Committee, Architectural Review Board, system consolidations, project implementations or system decommissioning.

For more information refer to Attachment I - financials

17 APPENDIX – ATTACHMENTS

The following attachments provide supporting information and lower level detail related to the ICT Strategy:

- ATTACHMENT A - Commonwealth ICT Benchmark spend report
- ATTACHMENT B - Capability maturity diagram – current and target state
- ATTACHMENT C - Capability maturity management plan
- ATTACHMENT D - Business unit plan review
- ATTACHMENT E – IT Roadmap on a page
- ATTACHMENT F - IT Strategic Initiative Summaries
- ATTACHMENT G - System health dashboard – diagram
- ATTACHMENT H - System health dashboard – table
- ATTACHMENT I – Financials
- ATTACHMENT J – Initiative Financials

Department of Justice

Prepared by Michael Hall and Melissa Lukianenko