PARLIAMENT OF TASMANIA

PARLIAMENTARY STANDING COMMITTEE OF PUBLIC ACCOUNTS

Follow-up of the Report of the Auditor-General

ICT Strategy, Critical Systems and Investment

(No. 4 of 2020-2021)

Members of the Committee

Legislative Council

Hon Ruth Forrest MLC
(Chair)

Hon Luke Edmunds MLC

Hon Bec Thomas MLC

House of Assembly

Mr Simon Behrakis MP
(until 11 June 2025)

Mr Roger Jaensch MP
(from 9 September 2025)

Mr Mark Shelton MP
(until 11 June 2025)

Mr Marcus Vermey MP
(from 9 September 2025)

Mr Josh Willie MP
(until 11 June 2025)

Mr Dean Winter MP
(from 9 September 2025)

Table of Contents

Charter of the Committee

The Public Accounts Committee (the Committee) is a Joint Standing Committee of the Tasmanian Parliament constituted under the *Public Accounts Committee Act 1970* (the Act).

The Committee comprises six Members of Parliament, three Members drawn from the Legislative Council and three Members from the House of Assembly.

Under section 6 of the Act the Committee:

- **must** inquire into, consider and report to the Parliament on any matter referred to the Committee by either House relating to the management, administration or use of public sector finances, or the accounts of any public authority or other organisation controlled by the State or in which the State has an interest, and

- **may** inquire into, consider and report to the Parliament on any matter arising in connection with public sector finances that the Committee considers appropriate, and any matter referred to the Committee by the Auditor-General.

Abbreviations and Acronyms

CIO	Chief Information Officer
DECYP	Department for Education, Children and Young People
DPAC	Department of Premier and Cabinet
DSAG	Digital Services Advisory Group
DSDSC	Deputy Secretaries Digital Services Committee
DSS	Digital Strategy and Services
HRIS	Human Resources Information System
ICT	Information Communications and Technology
MLC	Member of the Legislative Council
MP	Member of Parliament
NRE	Department of Natural Resources and the Environment Tasmania
PSPF	Protective Security Policy Framework
SIIRP	Structured Infrastructure Investment Review Process
TASGRN	Tasmanian Government Radio Network
The Act	*Public Accounts Committee Act 1970*
The Committee	Parliamentary Standing Committee of Public Accounts
WHS	Work Health and Safety

Executive Summary

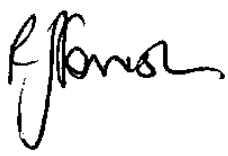
In 2020-21, the Auditor-General examined whether the Tasmanian Government's approach to ICT strategy, critical systems and investment was managed in an effective, coordinated and strategic manner. The audit identified significant gaps in whole-of-Government ICT governance, asset management and investment prioritisation, and made seven recommendations directed at the Department of Premier and Cabinet (DPAC), the Digital Services Board and agencies.

The Committee undertook this follow-up review to assess the extent to which those recommendations have been implemented. In doing so, the Committee wrote to the responsible Minister, received a written submission from DPAC, and conducted a public hearing on 5 February 2026 with the Minister for Innovation, Science and the Digital Economy, the Chief Information Officer and senior DPAC officers.

The Committee found that meaningful progress has been made since 2020-21. The Government has developed a whole-of-Government digital strategy, Our Digital Future, and an accompanying Strategic Action Plan. ICT governance has been substantially reformed, with the Digital Services Board replaced by the Data and Digital Subcommittee of the Secretaries Board, which now provides regular oversight of cross-agency digital priorities. Government ICT investment has more than tripled, rising from $26.5 million in 2021 to $93.8 million in the current budget. All agencies now maintain ICT critical asset registers, and a number of significant digital transformation programs are underway across Government.

However, the Committee also found that consolidation of asset information at a whole-of-Government level remains incomplete. A comprehensive view of critical ICT assets - encompassing age profile, interdependencies, risk exposure and replacement timelines - across all agencies has not yet been achieved. Work to establish a whole-of-Government critical systems register is only now being initiated. Additionally, the outcomes of the whole-of-Government ICT vision and strategy are not systematically measured or publicly reported.

The Committee makes four recommendations directed at completing the whole-of-Government asset assessment, establishing consistent asset register standards based on the Department of Health model, progressing the whole-of-Government critical systems register, and requiring DPAC to report publicly on ICT strategy outcomes through its annual report.



Hon Ruth Forrest MLC
Chair

25 March 2026

Summary of Findings

The Committee made the following 16 findings:

Area	Finding
AGR 1 **The Government enhance ICT investment evaluation and prioritisation by developing, through its current ICT framework, a whole-of-Government ICT vision informed by an understanding of each agencies [sic] key ICT assets, their age profile, key risks, interdepartmental reliance and proposed replacement timetable. This vision, and the strategy to implement it, should be developed as a priority. It should be delivered and executed within the next 18 months**	F1. Progress has been made toward Recommendation 1, however there is still work to do to understand the key ICT assets, their age profile, key risks, interdepartmental reliance and proposed replacement for each agency. F2. The Government ICT vision and strategy have been developed as reflected in 'Our Digital Future: Tasmanian Government strategy for digital transformation' and 'Our Digital Future: Strategic Action Plan' documents. F3. The changed operating environment under COVID-19 pandemic, and the additional resources made available, accelerated progress towards achieving a whole-of-Government ICT vision and strategy.
AGR 2 **The whole-of-Government ICT vision and strategy identify:** **a. key priorities for the short, medium and longer term** **b. strategies for greater collaboration targeting cost efficiency gains, increased productivity, removal of duplication of effort across agencies and alignment to Government strategy and policy** **c. known key ICT assets targeted for replacement or renewal, and** **d. critical assets that are significantly aged or at potential risk of failure.**	F4. Whole-of-Government ICT governance and planning are in place and maturing to ensure the ICT vision and strategy is delivered. F5. The Data and Digital Sub-committee has developed an annual work program that provides whole-of-Government oversight of ICT risks and opportunities. F6. Agency level planning in ICT strategy and key asset management is occurring. However, consolidation at a whole-of-Government level is incomplete. F7. It is unclear how the outcomes of the delivery of the whole-of-Government ICT vision and strategy is or will be measured and reported.
AGR 3 **The Government review the terms of reference for the Digital Services Board (DSB) to ensure it has the mandate to better support a prioritised and collaborative approach to ICT across agencies with DSB providing support and guidance, where needed, to agencies for ICT strategic planning and management of critical assets.**	F8. The Government has reviewed the terms of reference for the Digital Services Board and it is reviewed annually.
AGR 4 **The Digital Services Board to review implementation of the whole-of-Government ICT strategy to ensure it supports the Government's ICT vision and ensure plans are developed to implement the strategy.**	F9. Through the Digital Services Board, the Government has provided plans and is continuously reviewing the implementation of the whole-of-Government ICT vision and strategy: this work is ongoing.
AGR 5 **Agencies proactively plan and prioritise long-term, large scale and high value key ICT asset investment more effectively by improving**	F10. Whilst accepting the Auditor-General's recommendation in principle, the implementation of the whole-of-Government approach has taken a 'modern and contemporary approach' to ICT

Area	Finding
their understanding of their current ICT environments and collaborating where mutual benefits exist.	planning and investment by the Digital Services Board.
AGR 6 **The Department of Treasury and Finance revisit the feedback approach for Structured Infrastructure Investment Review Process (SIIRP) submissions to better inform agencies on areas for improvement for future SIIRP submissions.**	F11. Improved guidance on how to engage with the Structured Infrastructure Investment Review Process has occurred with a positive outcome. F12. In 2023 DPAC Digital Strategy and Services initiated work to review the Treasury guidance and explore practices relating to ICT investment funding and assurance used in other jurisdictions: this work has not been completed.
AGR 7 **Agencies maintain up-to-date ICT critical asset registers in a consistent format which identify key risks replacement dates and level of funding required.**	F13. In 2024 the Department of Health initiated a program to enhance its ICT asset register by mapping the interlinked asset dependencies for the agency. F14. The Data and Digital Committee resolved that Department of Health approach and the platform being used to accomplish the capability could be utilised by all agencies to enhance visibility of critical assets and assist to manage investment lifecycles. F15. All agencies now have up-to-date ICT critical assets register. It is not clear whether they are of a consistent form. F16. The Data and Digital Committee agreed to add a project to 2025 Data and Digital Committee Work Plan to explore the establishment of a whole-of-Government critical systems register, with a view to extend the register into an investment planning.

Summary of Recommendations

The Committee makes the following four (4) recommendations to the Government:

Area	Finding
AGR 1 **The Government enhance ICT investment evaluation and prioritisation by developing, through its current ICT framework, a whole-of-Government ICT vision informed by an understanding of each agencies [sic] key ICT assets, their age profile, key risks, interdepartmental reliance and proposed replacement timetable. This vision, and the strategy to implement it, should be developed as a priority. It should be delivered and executed within the next 18 months**	R1. The Government ensure progress continues to be made on the whole-of-Government understanding of the key ICT assets, their age profile, key risks, interdepartmental reliance and proposed replacement for each agency.
AGR 2 **The whole-of-Government ICT vision and strategy identify:** **a. key priorities for the short, medium and longer term** **b. strategies for greater collaboration targeting cost efficiency gains, increased productivity, removal of duplication of effort across agencies and alignment to Government strategy and policy** **c. known key ICT assets targeted for replacement or renewal, and** **d. critical assets that are significantly aged or at potential risk of failure.**	R2. Outcomes of the delivery of whole-of-Government ICT vision and strategy being reported by the Department of Premier and Cabinet in its annual report.
AGR 7 **Agencies maintain up-to-date ICT critical asset registers in a consistent format which identify key risks replacement dates and level of funding required.**	R3. As supported by the Data and Digital Committee, all agency ICT critical asset registers be consistent with the Department of Health template approach to mapping the interlinked asset dependencies. R4. The Data and Digital Committee continue to explore the establishment of a whole-of-Government critical systems register.

Conduct of Review

In line with section 6(2) of the Act, the Committee resolved to undertake a review of the responses to the Auditor-General's recommendations contained within Report No. 4 of 2020-21 – Information and communications technology, critical systems and investment.[1]

On 29 May 2025, the Committee wrote to Hon Madeleine Ogilvie MP (then Minister for Innovation, Science and the Digital Economy) informing her of the Committee's intention to follow-up the Auditor-General's Report with a questionnaire to establish the extent to which the recommendations of the audit had been implemented by the Tasmanian Government and the Digital Services Board. The original response deadline was set to 27 June 2025.

For each of the audit recommendations, the Committee requested a written response by the Department detailing actions undertaken to implement the same, including (but not limited to):

1. clear indication of acceptance, in part, in full or in-principle or non-acceptance for each recommendation
2. in the case of recommendations not fully accepted, the rationale for not implementing or otherwise adopting the recommendation and detailed explanation related to this decision
3. evidence of implementation or progress toward the implementation of each accepted recommendation
4. an explanation for any delay in the implementation of any accepted recommendation, and
5. any other relevant detail.

Copies of documents that provided evidence to support the responses to the recommendations were encouraged.

On 11 June 2025, Her Excellency the Honourable Barbara Baker AC (Governor of Tasmania), agreed to Hon Jeremy Rockliff MP (Premier) request to prorogue the Parliament and dissolve the House of Assembly and a State election was called for 19 July 2025.

Noting the existent care-taker period, the Committee Secretary and Departmental representatives renegotiated a revised response date, and a submission was provided to the Committee on 28 July 2025.

After the commencement of the 52nd session of Parliament, the Committee was re-established on Wednesday, 24 September 2025.

The Committee resolved to hold a public hearing with the responsible Minister and Departmental representatives in Committee Room 2, Parliament House, Hobart:

[1] See https://www.audit.tas.gov.au/wp-content/uploads/ICT-Strategy-Report-Final-Report.pdf

Thursday, 5 February 2026
Hon Madeleine Ogilvie MP **Minister for Innovation, Science and the Digital Economy** Department of Premier and Cabinet Representatives **Dr Justin Thurley (Chief Information Officer)** **Ms Noelene Kelly (Deputy Secretary)**

Copies of the transcripts, tabled papers, broadcasts and responses are available on the Committee's inquiry webpage.[2]

---

[2] See in general, 'Follow-up Audit: ICT Strategy, Critical Systems and Investment', https://www.parliament.tas.gov.au/committees/joint-committees/standing-committees/public-accounts-committee/inquiries/follow-up-audit-ict-strategy,-critical-systems-and-investment

Background

The Auditor-General undertook an independent assurance audit of the State Government's Information and Communications Technology (ICT) Strategy, Critical Systems and Investment.

The objective of the audit was to express a reasonable assurance opinion on whether Government ICT strategy, critical systems and investment were managed in an effective, coordinated and strategic manner.

The audit covered the following agencies:

- Department of Premier and Cabinet (DPAC), including the Digital Strategy and Services (DSS) Division
- the former Department of Communities Tasmania
- the former Department of Education (now Department for Education, Children and Young People - DECYP)
- Department of Health (including the Tasmanian Health Service)
- Department of Justice
- Department of Police, Fire and Emergency Management
- the former Department of Primary Industries, Parks, Water and Environment (now Department of Natural Resources and Environment Tasmania - NRE)
- Department of State Growth, and
- Department of Treasury and Finance.

The Report contained seven (7) recommendations against five (5) audit criteria:

1. Did the Government have a strategic approach to ICT governance and decision-making across the government that is coordinated and effective?
2. Have agencies prepared and maintained contemporary ICT Strategic Plans?
3. Have agencies managed key ICT assets that are vital for service delivery effectively?
4. Has the Government facilitated an investment evaluation and prioritisation approach to ICT investment that is effective?
5. Did the Government and agencies have plans to provide a pathway to digital capabilities?

In response to the Committee's request for an update, DPAC stated the following:

> *… Work relating to the ICT Strategy, Critical Systems and Investment Audit commenced in 2019 with the final report being published in August 2020. As this audit was progressing two initiatives were underway that were also significant for digital and ICT in government – the Tasmanian State Service Review and the development of Our Digital Future. Further complicating matters, all three activities occurred during the COVID-19 pandemic.*
>
> *The convergence of the Audit with the other three activities heavily influenced Government's response to the Audit recommendations, which are well summarised in the*

report's Executive Summary under the heading of "Collective response from Digital Services Board members" (pp8).

The Government's experience of the COVID-19 pandemic and its impact on Tasmanians reinforced the need for government to focus on digital services; to understand user needs and design and deliver accessible 'anytime, anywhere' services to protect Tasmanians and strengthen our economic recovery.

As a consequence, some of the recommended actions from the ICT Strategy, Critical Systems and Investment Audit were absorbed by Our Digital Future and the associated strategic action plan, and the digital reforms recommended in the final report of the Tasmanian State Service Review. In fact, the recommendations of the ICT Strategy, Critical Systems and Investment Audit were referenced as informing the recommendations Tasmanian State Service Review.

Our Digital Future has been instrumental in driving a range of strategic digital and ICT investments that have delivered tangible benefits to the Tasmanian community. These achievements demonstrate the government's commitment to its digital transformation agenda and its ability to translate strategy into action.

The ongoing contribution of the Data and Digital Subcommittee, which was established via recommendations 24 and 25 of the Tasmanian State Service Review, also remains central to digital governance. Replacing the Digital Services Board as a standing subcommittee of the Secretaries Board, the Data and Digital Subcommittee provides continuous oversight of whole-of-Government digital priorities, facilitates cross-agency coordination, and supports consistent data governance and information-sharing practices.

In addition to the whole-of-Government impacts, agencies have also actively progressed digital transformation initiatives aligned with core business priorities. The collective momentum of these efforts, illustrate the diverse ways in which Government has adopted new digital and ICT technologies to improve operations and service delivery...[3]

The Department also provided copies of supporting documents: see 'Summary of Attachments'.

At the public hearing, Minister Ogilvie elaborated further on actions taken:

***Ms OGILVIE** -... the ICT audit's focus on strengthening cross-agency digital infrastructure was directly reflected in Our Digital Future's strategic priorities. Similarly, the Tasmanian State Service Review adopted the audit's emphasis on unified governance and oversight, resulting in the establishment of the data and digital subcommittee, which now oversees whole-of-Government digital priorities and facilitates cross-agency planning and coordination. These and other reforms have strengthened whole-of-Government oversight, prioritisation and delivery of data and digital initiatives.*

[3] Letter from Shane Gregory (Associate Secretary, DPAC) to Committee dated 28 July 2025, Attachment A

Since 2020-21, the Government has more than tripled its investment in ICT programs. This is guided by strategic planning at both the agency and whole-of-Government levels. Our Digital Future has also been instrumental in driving a range of strategic digital programs and ICT investments that have delivered tangible results and benefits to the Tasmanian community.

An increased number of ICT initiatives have progressed through the Structured Infrastructure Investment Review Process, which we all know as SIIRP: and agencies now maintain critical ICT asset registers, helping Government to build a more consistent and unified overview of its critical assets. These outcomes demonstrate our Government's commitment to its digital transformation agenda and our ability to translate strategy into action.

Just a little bit on the numbers: Government has more than tripled its investment in ICT programs since 2021, with investment up from $26.5 million in 2021 to $93.8 million in the current budget. That's a year-on-year increase from 2.5 per cent in 2021 to 11 per cent in the current budget. ...[4]

---

[4] See Public Hearing (5 February 2026) - Min Ogilvie, https://www.parliament.tas.gov.au/__data/assets/pdf_file/0015/101832/PAC-Follow-Up-Audit-ICT-Strategy-Critical-Systems-and-Investment-5-February-2026.pdf, p.1-2

Departmental Responses

Auditor-General Recommendation 1

The Government enhance ICT investment evaluation and prioritisation by developing, through its current ICT framework, a whole-of-Government ICT vision informed by an understanding of each agencies [sic] key ICT assets, their age profile, key risks, interdepartmental reliance and proposed replacement timetable. This vision, and the strategy to implement it, should be developed as a priority. It should be delivered and executed within the next 18 months[5]

DPAC reported to the Committee it had accepted the Auditor-General's recommendation in principle:[6]

> *The Digital Services Board audit response, published in the final report outlined the boards position in relation to work that was already underway developing the Government's Digital Strategy, Our Digital Future.*[7]
>
> *The Board accepted the recommendation in principle but tempered the proposed response, indicating that "it would be inappropriate for the Government to define an ICT strategy or vision in the absence of a digital vision and strategy", and that Our Digital Future specifies the development of a whole-of-Government technology roadmap as a strategic action and this body of work would address Recommendations 1 and 2 of the Audit.*

DPAC provided the following as evidence of implementation or progress (continuous delivery):

> *Our Digital Future was released in June 2020 and this strategy set a broader strategic context for digital transformation and articulated the government's commitment to leveraging digital technologies to improve the lives of Tasmanians, drive economic growth, and enhance public service delivery.*
>
> *Later in 2020 and also accounting for urgent actions required to support the COVID-19 recovery, Government release the Strategic Action Plan supporting Our Digital Future.*[8]
>
> *Under the digital government workstream, an action was included to develop a whole-of-Government technology road map.*
>
> *Critically the development of this roadmap for whole-of-Government has been largely subsumed into the annual Data and Digital Subcommittee Work Plan,*[9] *it is also recognised that the pragmatic development of detailed technology roadmaps is undertaken by system owners and those who deliver the systems working in alignment*

[5] From the date of the original Report that was tabled 27 October 2020, this would suggest delivery and execution to have been completed by end of April 2022
[6] See Attachment A, p.3
[7] See Attachment B
[8] See Attachment C
[9] See Attachment D

with government digital priorities, directions and standards (whole-of-Government or within agencies).

DPAC pointed to Attachments B to D as supporting evidence for this recommendation.

At the public hearing, with respect to Recommendation 1, Minister Ogilvie and Dr Justin Thurley (Chief Information Officer, DPAC) provided the following:

***Ms OGILVIE** - ... In relation to Recommendation 1, which is whole-of-Government ICT vision and investment prioritisation, while the 2020 audit identified gaps in ICT strategy and planning, our Government has delivered a clear digital direction through that Our Digital Future Strategy that I spoke of earlier and its accompanying strategic action plan. Our Digital Future was released in June 2020, setting out our strategic direction for digital transformation and our commitment to improving services, economic opportunity and outcomes for Tasmania.*

Following the pandemic, the strategic action plan was released to accelerate digital initiatives, including the development of a whole-of-Government technology road map to really guide that ICT investment, our modernisation and to help prioritise those activities. Many elements of the road map have since been incorporated into the annual work program of our data and digital sub-Committee, which is a good thing, ensuring alignment between strategic direction and practical delivery within Government.

The whole-of-Government ICT investment is now guided through a strengthened digital governance model centred on the data and digital Committee. That's at the heart of the organisational strategy and its work plan. This provides, we think, clearer oversight, prioritisation and better alignment across Government agencies…

***CHAIR** - From my perspective, there's a number of areas the Auditor-General pointed to, like each agency's ICT assets, their age profile, key risks and interdepartmental reliance on the proposed replacement timetable. I know you have increased the investment in ICT. ...*

***CHAIR** - ... When I went through the information provided, it wasn't clear to me - and this may be covered better under another recommendation, whether or not you have all the critical assets across each department and agency. Or is that still a work in progress? ...*

***Dr THURLEY** - ... I will go back to the idea of the in-principle agreement of the recommendation. I think that the big difference is that we, as a Government, agreed on the intent of the audit. But the particular mechanisms that were put into the recommendations, we didn't necessarily agree with the way forward, particularly in the contemporary way and with the changing nature of digital and ICT, particularly during the pandemic and then post the pandemic as well. It really was a bit of a reform for us.*

Not only that. The reforms that we identified through the State Service Review and the work that was done in this particular work with Our Digital Future, we identified that to make the strategy work properly, we need good governance. Governance is part of the recommendations further on, but it is something that was completely overhauled and through the secretary's board, we established a subcommittee of Government called the

Data and Digital Committee that was given the remit of oversight of whole-of-Government activity and to coordinate the agencies around their risks and their ICT policies and also to collaborate on projects and initiatives that were core or common across Government.

***Mr WINTER** - ... Is it the Government's view that we're heading towards a whole-of-Government ICT department? As I understand it, every department still has its own IT team managing its own IT environment. You talked a little about a collaboration between departments where they can, which is good, but is it the Government's view that at some point in time we need to bring things together under a single entity, or are we going to continue with the separated model?*

***Ms OGILVIE** - ...We operate in a matrix environment and it's one of the questions that every large organisation has about the value of centralisation versus a more matrixed and distributed model. It is really helpful for our departments to have capacity in their departments to be at the front line to manage and deploy information IT projects, et cetera, and to understand what's happening at that front line and be able to feed that back up the food chain.*

We have Dr Thurley here, who is the CIO who sits right across all of that. Sorry if I'm going too far, but Dean, I suspect part of your question is about the funding line and being able to map where the spend sits and goes within each department. I think that question which has been raised over many years is one for the CIO because it's also with Treasury as well, but what I will say is, given the matrix environment that we operate in at the moment, the institution of the Data and Digital Committee that we have now has helped to smooth conversations across divisions, which is really helpful, so those whole-of-Government-type projects, and we're seeing some dialogue around the AI issue at the moment that are going to affect everybody, are about how we best manage that and make sure we're deploying that safely and well across all departments. ...

***Dr THURLEY** - ... The current Data and Digital Committee has all the CIOs across the agencies in one place, so we have everybody in the digital and ICT space, but we also include a number of other stakeholders who have different standings in terms of how our work is impacted or that we need their support or advice to move a lot of the whole-of-Government things together. We also include people from the Office of the Solicitor-General and some information management specialists as well.*

To the heart of the question that was asked - the centralisation versus decentralisation issue - I won't go into opinions because I can't, but I can certainly put on the table where Government policy sits at the moment and how we achieve the sort of centralisation that is part of some of our success.

At the moment, it is Government policy that there's autonomy within the agencies and it's into the management and accountabilities of risk. I won't go further into that because I think it's pretty well understood how that works, and that does change some nuances in terms of how you have to manage what priorities across agencies, so they're different across agencies, but at the same time we understand we have a lot of commonality and a lot of things that we do would benefit from sharing capability, which is something the

Tasmanian Government is very good at, even though we're not fully centralised like some of the other jurisdictions.

The way we achieve that is we have digital strategies and services within DPAC, which provides a range of shared infrastructure services, and we also look after shared common systems across Government, but not all of them. For example, Networking Tasmania and the networks the Government and this establishment relies on, is all part of a central whole-of-Government network. That's something that no other state in Australia really has to the extent that we have. That's all shared and managed out of DSS.[10] We also have examples that we deal with. We manage telecommunications and communications in general, all the communication services, all through DSS as a central and shared service. We also provide other services to Governments such as the HR system and we look after the fines management infrastructure. There's a range of other services. I won't go into every one of them -

***Mr WINTER** - Is the HR system you mentioned the HRIS?[11]*

***Dr THURLEY** - That's the HR Empower system, which is the current legacy HR system. DPAC is also undertaking the whole-of-Government HR transformation, which is the HRIS which will replace that system and will assume similar sorts of shared capability across Government.*

***Mr WINTER** - Is it the intention that that will oversee all departments?*

***Dr THURLEY** - It is the intention.*

***Mr WINTER** - How far progressed is that?*

***Dr THURLEY** - Substantially, without going into the -*

***CHAIR** - It's been having a very long gestation, this one.*

***Mr WINTER** - Is it still in the Department of Health?*

***Dr THURLEY** - No, it's been transferred to the Department of Premier and Cabinet.*

***Mr WINTER** - It hasn't been rolled out in Department of Health?*

***Dr THURLEY** - Parts of it have been rolled out in the Department of Health. The Department of Health started the process. We have then picked it up to make it go whole-of-Government.*

***Mr WINTER** - The Department of Health commenced the project but didn't see it to the end and instead transferred it to DPAC. Is that now under your area or a different part of DPAC? ...*

[10] Digital Strategy and Services
[11] Human Resources Information System

Dr THURLEY *- The HRIS has been transferred to the Department of Premier and Cabinet with the view that we have the services and capabilities to take that across Government. It's sort of part of DSS's bread and butter, but there is also a dedicated program team that sits within DPAC that is actually moving that transformation along. I just want to emphasise that the transformation is not just systems and software, it's about the people and change across the Tasmanian State Service. It's a fairly significant piece of work and a bit of change management. Software is only part of the equation and there's quite a bit of work involved to move that along. At the moment the focus is on the organisation and the human capital management component in that software.*

Mr WINTER *- Just so I'm really clear, HRIS is intended to be whole-of-Government. It started in Health, it's now gone to DPAC where it will be rolled out first.*

Dr THURLEY *- Whole-of-Government.*

CHAIR *- It wasn't made live in Health, though - or was it?*

Dr THURLEY *- There are elements of it that are live in Health, but not all parts of it are live, if that makes sense.*

Ms THOMAS *- Is it just human resources?*

Dr THURLEY *- I emphasise that it's a broad level. It is human resources, but it's the broader area of domain of room and resources which would include WHS,[12] safety, et cetera. It also includes rostering and payroll and human capital management.*

Ms THOMAS *- But not information management.*

Dr THURLEY *- Information management associated with people, yes.*

...

Mr WINTER *- Out of the auditor's report, it said there was no comprehensive information from agencies supporting the whole-of-Government framework for informing investment priorities, nor was there a comprehensive approach to identifying shared functionality such as human resources or finance, where more effective and efficient service delivery could be achieved. If we're talking about the response to this report, governs our moves to having a focus on deploying a whole-of-Government HR system, which is HRIS, what's the timeline for implementing HRIS across the department?*

Dr THURLEY *- The timeline for the HRIS at the moment is through the next two years. In the budget papers you can see where the dollars are going and what's happening with that. There is an active program with associated governance which is across the secretary's board and down into the various Committees that need to basically run the programme like that. That includes the likes of commercial aspects of it, the system roles and ownership.*

[12] Work Health and Safety

We also have the implementation program which is going ahead right as we speak. We also have the other components that need to be planned and mapped out. It's part of a broader road map for the overall program. That includes the likes of rostering, when we get it, how it goes in, the WHS and how we get the safety systems in and working. They can be somewhat run independently, but they're all dependent on the core: so, you can understand that there's a two-year remaining program to get this work ahead. What happens is, as the project progresses, we will obviously have understanding updates, and we plan on implementing payroll in two years' time.

...

***CHAIR** - Back to what Dean alluded to on centralisation rather than partial decentralisation. How do you then avoid duplication in that model? We all know that in the past we've had ticketing systems put in place that have cost many more millions of dollars than expected, and then someone else does it, whether it's a GBE[13] or whoever. What's the process there to avoid duplication under the current model?*

***Dr THURLEY** - The Data and Digital Committee meets once a month. That Committee has remit and a road map - not so much a road map, but a work plan - that actually looks at various objectives we have at a whole-of-Government level, which gives the opportunity, when you go through a planning process, just like many people would plan -*

***CHAIR** - Is that the one that was provided to us?*[14]

***Dr THURLEY** - Yes, that's a 2025 one, or earlier: and we've just completed today and gone through the new iteration of that. Typically, what we put on there is where we see systems that are either core systems to Government and any changes that we're making to them, and/or if there are new systems coming on board in other agencies we think can reduce duplication, if it's the right word, we talk about whether we put them on the list for oversight or whether we are supporting them in some way.*

For example, there might be an identity management system being implemented in the Department of Health. We will know through the conversations we have, and we are continually updating our conversations every month about what systems are coming on, what new procurements they might be making. Then we can look at them and say, that's something our department or another department wants to solve.

***CHAIR** - They don't actually go to full procurement until they've run it through this Committee? They don't go off on a frolic of their own?*

***Dr THURLEY** - That's right, it's a very collaborative and standard approach. I guess we have to be understanding the agencies need to produce outcomes aligned to their accountabilities and risks. However, it is very clear, and made very clear during our meetings, what activity is undertaken in those departments, and if there's anything new coming up, we would know about it.*

[13] Government Business Enterprise

[14] See Attachments H and I

It's a jurisdictional thing for us that we're actually fairly - as I said, it's a Tasmanian thing too - we're very close together to be able to work together. We share the information quite readily. We meet every week in a stand-up meeting to discuss the issues and if there are new things we need to bring onto the table we will bring them up.

Questions were asked about the Justice Connect Astria project referencing information online:

Ms THOMAS *- ...*

> *The Tasmanian Department of Justice's $35.2 million Justice Connect Astria is a major IT overhaul aimed at replacing outdated paper-based and manual systems with an integrated end-to-end digital solution. In 2023, Audit Tasmania noted that the project was not initially effectively planned and monitored for benefits realisation.*

Maybe it's the topic of another audit report that needs follow up, if there's one: but is that separate to this HRIS system, both very significant investments of taxpayer money? Are they for different purposes and both though seem to have faced really complex rollouts and delays?
...
Dr THURLEY *- You've actually brought up a really good point. Yes, Justice Connect* [is] *for a different purpose for identifying ... a whole range of systems that needed to be replaced and integrated. The system is complex, I will give you that. It is a very complicated process but it also it's been very successful at bringing systems together and centralising a lot of the work that's been done around the core systems that Justice needs to operate on.*

That was one of the programs that was invested in and through the broad level thinking across Government to say we do understand that Justice is doing this work - what type of work they're doing. They obviously brought in people from different agencies to help with the governance of it once we ran into a few little hiccups and things. I think it's a good example of that we understand that the how the assets are replenished - the life cycles are addressed - the loss of users are addressed. Also, that it is actually that particular program is a Justice specific - capabilities that are being addressed in in that space.

Ms THOMAS *- Will they also use HRIS alongside that?*

Dr THURLEY *- Yes, they will. There's no overlap realistically apart from potentially identity within the HRIS being the system of record for employees.*

The Minister was asked about the asset replacement schedule in place:

CHAIR *- ... have you really clear oversight of all departments and agencies, key assets, their age and status of them and a replacement schedule or whatever?*

Dr THURLEY *- ... this is a journey that we've been on since this audit and obviously it is clear to understand what your assets are and what replacement cycles you need. Again, just to get into focus here - was really the agencies, because of that autonomy and the risk*

appetites and everything being controlled at agency level, we needed to make sure the agencies were undertaking that type of work.

There's been an absolute concerted effort by every agency in the Tasmanian Government to get their - what I would probably more refer to as ICT infrastructure planning - under control and build those asset lists and know what their assets are. There's been different approaches taken in different departments. I understand and acknowledge the auditor raised that. At the same time these were necessary for the type of systems et cetera they are running.

For example, in Health there are some complexities and information that you must be aware of and involved in versus say something you might have in DPAC - there'd be less information held about a particular attribute of a system. You will see that there's some nuanced part of it.

What was really critical to us was to say you are all doing this and you're actually getting this done and we've got evidence of it. We'd actually provide some evidence to the Committee on that. Probably it's actually enabled us once we've got to this stage of maturity in handling it we're actually about to take the next step, which is actually to really focus on what intent the auditor wanted. Do we know what's critical across all of Government?

***CHAIR** - Do you?*

***Dr THURLEY** - Yes. Well, to an extent that we understand where the pinch points are. We've got some issues, in fact it's very connected to how we do cybersecurity as you can imagine. We have just recently last year initiated a program to look at what we would describe as the critical assets of Government or systems of significance to Government. So that we can actually get on top of - at a whole-of-Government level - of understanding where really are the crown jewels of all the Government. What are the asset issues we might have and how does that with other system dependencies [interact]?*

We have started that process now we're about 85 per cent through getting to a point where we can say what the lifeline services are for Government and say what the critical assets, ICT assets are that are connected to those services. Therefore, we can actually employ a range of risk management controls including, do your replace assets that are, out of date or is that one a cybersecurity one we need to really focus on keeping it protected, et cetera - there's a range of benefits.

...

***Mr WINTER** - How much of that is moving from physical infrastructure to cloud-based and is that a part of the strategy?*

***Dr THURLEY** - ... Migration from on-premises to cloud has been a big part of a lot of our work in recent years. From back in 2020 we established the 'cloud policy' and it's still there in place. We're probably looking to review that now because there's been massive transition into cloud-based services. ... - it de-risks a lot of what we do, but it also introduced new types of risks that we are actively managing.*

Mr WINTER *- Does that still include the on-island cloud preference, or has that gone now?*

Dr THURLEY *- No, that preference was removed from the policy. I can't remember what date it was, but yes, for obvious reasons.*[15]

Committee Findings

F1. Progress has been made toward Recommendation 1, however there is still work to do to understand the key ICT assets, their age profile, key risks, interdepartmental reliance and proposed replacement for each agency.

F2. The Government ICT vision and strategy have been developed as reflected in 'Our Digital Future: Tasmanian Government strategy for digital transformation' and 'Our Digital Future: Strategic Action Plan' documents.

F3. The changed operating environment under COVID-19 pandemic, and the additional resources made available, accelerated progress towards achieving a whole-of-Government ICT vision and strategy.

Committee Recommendations

R1. The Government ensure progress continues to be made on the whole-of-Government understanding of the key ICT assets, their age profile, key risks, interdepartmental reliance and proposed replacement for each agency.

---

[15] See Public Hearing (5 February 2026) - Min Ogilvie, p.2-9

Auditor-General Recommendation 2

The whole-of-Government ICT vision and strategy identify:
a. key priorities for the short, medium and longer term
b. strategies for greater collaboration targeting cost efficiency gains, increased productivity, removal of duplication of effort across agencies and alignment to Government strategy and policy
c. known key ICT assets targeted for replacement or renewal, and
d. critical assets that are significantly aged or at potential risk of failure.

DPAC reported to the Committee it had accepted the Auditor-General's recommendation in principle, as per the reasoning provided under Recommendation 1.[16]

DPAC provided the following as evidence of implementation or progress (continuous delivery):

> *Establishment of the Data and Digital Subcommittee of the Secretaries Board and its annual work program addresses planning for the short-, medium- and longer-term whole-of-Government initiatives that are focused on collaboration, efficiencies and policy alignment.*
>
> *The 2024 and 2025 work programs have comprised five active work streams – Digital Services, Common Systems and Platforms, Data and Information Governance, Cyber Resilience and Risk, and Digital Workforce Capabilities.*
>
> *Agency ICT strategies and infrastructure plans address plans for assets primarily supporting agency outputs, although there are exceptions for shared capabilities and service across various agencies.*
>
> *Whole-of-Government digital infrastructure and common business systems are predominantly delivered by DPAC Digital Strategy and Services (DSS). DSS maintains detailed roadmaps and plans for those services.*
>
> *Similarly, addressing recommendations 5 and 7 has allowed agencies to progress the replacement and renewal of ICT assets and to help identify critical assets that are significantly aged or at potential risk of failure (see responses outlined for recommendation 5 and 7).*

DPAC relied upon Attachments B to I as supporting evidence for this recommendation.

At the public hearing, Dr Thurley and Ms Noelene Kelly (Deputy Secretary, DPAC) provided the following:

> ***CHAIR** - This is in response to Recommendation 2. You provided a number of examples of the work plan of the subcommittee, which we just referenced, and a number of agencies' plans. Are there any that are still outstanding that haven't done this work?*

[16] See Attachment A, p.4

Dr THURLEY *- Look, there'd be no one that hasn't done any of this work. It is more about the type and extent of that work. ...*

...

Dr THURLEY *- ... everybody has undertaken the planning processes.*

CHAIR *- Who hasn't completed the process?*

Dr THURLEY *- Completed the process? Everyone's completed a process, yes. And it's an ongoing, continuous process, as you can imagine. Every year we review it. Probably more often than that nowadays.*

CHAIR *- The initial assessment of what are significantly aged assets or at risk of failure, you could confidently say that across the whole of State Government, you're aware of where those pinch points are?*

Ms KELLY *- What my comment to that would be is that, that work that Justin was just talking about then at a whole-of-Government level, that's still underway. We don't have a document for example, that would say, 'Here's the 100 systems that Government has and this is the order of priority, and this is their legacy,' and so on. We've got that information from agencies and we're just working through now, at that whole-of-Government level. In regard to Recommendation 1, what I would say is there's still ongoing work in that particular recommendation.*

CHAIR *- Well, that's Recommendation 2 as well.*

...

CHAIR *- The plan is, then, to have that all sort of in one, I will call it 'document' for want of a better word, so that it's really clear what's out there, what's at risk of failure .... Then you will start the prioritisation after that? Or are you doing the prioritisation as you go?*

Ms KELLY *- My expectation is that we would be in a position where we can advise Government and advise Secretaries of the department about legacy and ageing infrastructure, and the risk associated with that, and to be able to give them advice based on the recommendation from the Data and Digital Committee about what priority order investments should be made, and the consequence if we don't.*

CHAIR *- What is the timeframe from having that sort of level of completion - well, the completion of one part of a whole ongoing process, obviously?*

Dr THURLEY *- ... The main thing is, if we identify a system that, you know, we say, 'Look, this is a risk to Government and needs to be replaced' or there's other issues with it, because that's not just about systems, and there's no life-cycle road map plan in place for that system, which I'd be very surprised about. But you can understand that there are complex systems in Government that actually do have some issues like that. The idea with that we would go through a process of understanding what the options are to move forward. Build a plan, business case with investment options for how to replace those systems. That's a very common approach that's done.*

It's done in different ways. It can be purely brought in as do the work and do a budget bid and say, 'Look, we need to replace the system. This is a risk to Government'. That process is well understood, and you've probably seen the evidence of that coming through.

There are also scenarios where we're not sure about what has to happen next and we need to run a bit of a process to understand that. Or we want to make some change to that investment, which we then use the Structured Infrastructure Investment Review Process (SIIRP) for, which is part of the Audit recommendations too. The SIIRP process gives us a chance to do the investment options, understand the business case and have a stage-gated sort of approach to say, 'We're off. Where do we go next? Is it an investment option here or is it that way? Or do we do nothing and decide to hold that risk?'

***Mr WINTER** - This audit you're doing of the infrastructure, is that directly responding to Recommendation 2, or is that something that has happened organically out of the other work you're doing?*

***Dr THURLEY** - This process is, I would say, not directly responding to this audit because we would say that the changes and reforms that we have undertaken since 2020 have brought us to a point where we have a more mature process for this. We've got to a point where we're actually saying, well, if we do this, we can have a range of outcomes for Government by going through this process. We're capable of delivering the information. ... we're actually able to use that information for a different range of purposes, not just for life-cycle planning but, potentially and more interestingly, for security and potentially for emergency management as well. You can see there's a range of spin-offs for us, and now we're in a really good position to exploit those capabilities that we've built.*

***CHAIR** - It will become easier, perhaps, to take a proactive approach rather than a reactive approach? If suddenly something fails or it's at imminent risk of failure, you will be able to identify those assets earlier and schedule replacement, or new systems, or whatever?*

***Dr THURLEY** - I will use an example of how powerful this can be. We have, in the Department of Health, and you can understand, a very complicated environment. They've initiated a program around their asset management to see those assets and those dependencies in real time. In other words, they know exactly where it's connected, what's happening at any point in time and they just show the dependencies all the way from the business service through to the end asset. That's ultimately the goal that we would like to see for all of Government. But, as you can imagine, that'd be complicated.*
...
***Dr THURLEY** - ... Having that in place and being able to take that type of approach to whole-of-Government would be a massive step forward. We see it from a security and observability point of view: that we can see what's going on before or as it's happening. It gives us a massive advantage in that space.*

As I said, to get to that point, we need to have invested in the capabilities at the low end, the ability to gather the information about those assets and technology from 2020, versus

where technology is in 2025-2026. There are capabilities now of those little agents that can gather up this information and help us with that automated data collection.

***CHAIR** - In the executive summary of the Auditor-General's report, he makes the comment:*

> *In our view, ICT investment, evaluation and prioritisation can only be considered effective where it is based on a vision that has been clearly defined, with key deliverables and outcomes which can be measured.*

How are you measuring success?

***Dr THURLEY** - I guess the measurement of the performance of success against our vision, I reckon it's an interesting challenge. We should be setting what we expect the situation to be in the future, i.e. the target state. For example, if I could use Our Digital Future as the most obvious example to use, how do we know that we've achieved those components? As you know, some of those components are actually quite complex. There are multiple initiatives to hit those measurements. We've been actively tracking Our Digital Future since that's been in play. We're just about to go through the process of refreshing that strategy. In doing so, we've also been able to say that we've hit a range of achievements. It's meeting the outcomes and achievements for each of those areas is how we kind of measure ourselves. Because we're talking about long periods of time here, we've just been trying to capture those achievements and to document them where possible. ...*

***CHAIR** - ... Documenting achievements. I will just go to one here on strategy, under the Government responsibility of the strategy:*

> *Develop digital culture and capability across Government agencies.*

How are you doing that and how are you measuring it?

***Dr THURLEY** - ... digital capability - one of the parts of the Data and Digital Committee's work plan was digital capability and workforce uplift. We actually had a number of initiatives that are in that space that were aimed at potentially more so building the skills of some of what I would call technical fluency with our professionals in that space, less so as the workforce in general, which is still a challenge and there's been massive inroads there anyway.*

The work that we've done there is about bringing capable people through, understanding their skills and knowing how to map those skills and address any of the gaps. Recent work we've done, it's hooked into the skills framework for the information age, which I am not sure if you're aware of, but it's an international standard for identifying skills and capabilities within the ICT domain, or, actually, digital domain. We've been actively working through those skills and mapping them to roles and then trying to find out where our gaps are to try and build out that, and initiate capability and uplift in that space.

***CHAIR** - I will go back to the question: how are you going to measure that you've actually achieved the intent?*

***Dr THURLEY** - Ultimately, we will be able to say that we can measure and map individuals against those skills in this instance. We can map those individuals against those skills and say that they've achieved those skills.*

***CHAIR** - They will be assessed in some way?*

***Dr THURLEY** - Yes, there is assessment. I put my emphasis on this: this is early stages, and it's not done in every domain of ICT yet.*

***CHAIR** - Clearly, if people are digitally literate and smart, they're less likely to breach some IT-important protocol and bring down a whole system or something, or at least even not being hacked or clicking on a link that you really shouldn't have done.*

***Ms KELLY** - ... an example of that might be Cyber Awareness Month, which is held in October every year, and because DSS has responsibility for whole-of-Government cyber, they work really closely with the agencies to deliver training programs during that month. It's not to say that that's the only time they do it, but for example, in our department, Department Premier and Cabinet, we also have ongoing cyber programs where, for example, we have those phishing exercises, so we might get an email out of the blue that looks okay but we're able to assess behind if employees click on certain links and don't mark it as phishing -*

***CHAIR** - So you do a little test.*

***Ms KELLY** - Yes, we do little tests quite regularly throughout the year. There are different opportunities particularly around security to provide training, but also to assess people's uptake of that as well.*

***CHAIR** - Going back to Our Digital Future, you've got the number of major actions in there across community, economy and Government. These are the things that you will be working to prepare performance measures against, or what? Again, I will go back to the outcomes focus here.*

***Dr THURLEY** - Yes. The question is ... have we met the outcomes of that particular action? We're often measuring it in terms of, in the first instance, did we execute something was going to make a difference, and then how do we know if that made a difference? I guess we look at things like are we - I'm trying to think of a good example in that group. For example, I think uplifting cybersecurity was one of the original actions in Our Digital Future.*

We have effectively ran through in the way we would - it's not just to put one measure on things, but have we increased our capabilities in that space and how do we do that? We've had independent reports to say this is where we've got to, this is how we've - how much we've increased our maturity. This is what systems with level capabilities we've left

in place so we know that we're actually starting to tick the boxes of that uplift. It's a very broad-level action that would have multiple performance capabilities in it.

***CHAIR** - How do you report your progress on these, ...*
...
***Dr THURLEY** - ... I will just emphasise the nature of the Our Digital Future being a broad level, economy-level strategy that looks at the role of all the players or stakeholders, including Government's role, the community's role and industry's role. Therefore, you're right, it's an ongoing component that you would expect all parties to be engaged in and what sort of engagement we have in getting initiatives on the table and out the door to deliver any sort of change in that digital inclusion space which we have started to move into. It's been a challenge for Tasmania, as has been documented, but we have run a range of activities and at the individual initiative level we would have reports that suggest this is the improvement, or this didn't work and this is the learning we got from it.*

***CHAIR** - You have engaged with the Department for Education, Children and Young People (DECYP) on this, obviously?*

***Dr THURLEY** - Just about every agency had something happening in that space, but DECYP was the largest area. Also, State Growth ran the Digital Ready for Daily Life. There's a range of programs all being delivered across the Government in different spaces.*

***CHAIR** - In terms of reporting against this, how do you report against it?*

***Dr THURLEY** - We're reporting against this through the tracking that I described. ...*

***Mr WINTER** - Do you report to, like, the agency Secretaries or the Minister or -*

***Dr THURLEY** - There has not been any direct [reports] on how that's going, because what we would say would be more reporting on the Government's actions that come out of it. For example, if it was an action that Government was specifically doing, like cyber uplift, I will just use that as an example, then we'd be definitely reporting through the governance about how we're achieving our outcomes for that project and that program which we have. The end-of-project report says what benefits were achieved, what outcomes we have and what learnings we had.*

***CHAIR** - ... Is this information available publicly or do you report this in your annual report, for example?*[17]

***Dr THURLEY** - No. We haven't put that publicly, but it has been the intent that we provide that highlights report as an example.*

***CHAIR** - In your annual report?*

[17] See Attachment K

Dr THURLEY - *Yes.*[18]

Committee Findings

F4. Whole-of-Government ICT governance and planning are in place and maturing to ensure the ICT vision and strategy is delivered.

F5. The Data and Digital Sub-committee has developed an annual work program that provides whole-of-Government oversight of ICT risks and opportunities.

F6. Agency level planning in ICT strategy and key asset management is occurring. However, consolidation at a whole-of-Government level is incomplete.

F7. It is unclear how the outcomes of the delivery of the whole-of-Government ICT vision and strategy is or will be measured and reported.

Committee Recommendations

R2. Outcomes of the delivery of whole-of-Government ICT vision and strategy being reported by the Department of Premier and Cabinet in its annual report.

---

[18] See Public Hearing (5 February 2026) - Min Ogilvie, p.9-14

Auditor-General Recommendation 3

The Government review the terms of reference for the Digital Services Board (DSB) to ensure it has the mandate to better support a prioritised and collaborative approach to ICT across agencies with DSB providing support and guidance, where needed, to agencies for ICT strategic planning and management of critical assets.

DPAC reported to the Committee it had accepted the Auditor-General's recommendation in principle:[19]

> *In its audit response the DSB advised that if a formal review of ICT governance was to be undertaken, it should be an end to end review and include the entire ICT governance framework including the Terms of Reference for both the Deputy Secretaries Digital Services Committee (DSDSC) and the role of the Digital Services Advisory Group (DSAG), noting that a biennial review was already part of the Terms of Reference of each of these governance bodies.*

DPAC provided the following as evidence of implementation or progress (completed in April 2022):

> *The ICT Governance Framework was subsequently reviewed and restructured in response to recommendations 24 and 25 of the Tasmanian State Service Review.*
>
> *In April 2022, the newly formed Tasmanian Government Secretaries Board established the Data and Digital Sub-committee comprising agency CIOs[20] and key information management stakeholders from across government.*
>
> *The endorsed role of the Data and Digital Subcommittee is to:*
> - *oversee whole-of-Government digital initiatives*
> - *monitor progress and the delivery of significant government digital priorities (including Our Digital Future)*
> - *lead engagement and collaboration across government agencies to promote a user-focused, and 'one government' approach to the design and delivery of digital services, and*
> - *facilitate the establishment of effective data governance and data sharing capabilities across government.*
>
> *The Terms of Reference are reviewed on an annual basis.*

DPAC relied upon Attachment J and Recommendations 24 and 25 in the *Tasmanian State Service Review*[21] as supporting evidence for this recommendation.

At the public hearing, Minister Ogilvie, Dr Thurley and Ms Kelly provided the following:

---

[19] See Attachment A, p.5
[20] Chief Information Officer
[21] See *Independent Review of the Tasmanian State Service Final Report (July 2021)*, Accessed at: https://www.dpac.tas.gov.au/divisions/policy/review_of_the_tasmanian_state_service/TSSR_Final_Report.pdf, p.134-137

CHAIR *- ... If we go to Recommendation 3 - this was with regard to the review of the terms of reference to the Digital Services Board. They provide a copy of the new terms of reference. Minister, do you want to speak any further to that? I'm particularly interested in the reporting of the subcommittee, how that goes. I believe that was covered a bit previously by the CIO.*

Ms OGILVIE *- ... I would also just like to share my understanding that as a Government, the digital and data skills and the capacity we have to help lift the workforce and digital inclusion and those elements, we take that very seriously as well.*

We are a large employer of digital and technology people and we see that quite a porous workflow of people has quite often spent time in Government so we do take very seriously our obligation to make sure that people's skills are developed. I'd like to get that on the record.

In relation to the Data and Digital Sub-Committee, I would like to get onto the record for you the endorsed role, what its role is, and that is to oversee whole-of-Government digital initiatives. We've heard some great discussion around what some of those initiatives are and how it's been an improvement to what had been occurring before. It monitors progress in the delivery of significant Government digital priorities, including Our Digital Future Strategy. This one, I think, is really important to lead engagement and collaboration across Government agencies.

We are very fortunate in Tasmania with two degrees of separation that we can work together, but as we see technology even accelerating in its advancement and our ability and our need to implement new systems and models, it is that collaboration that keeps us all on the same page, so I'm very grateful to everybody who's on that Committee and particularly our CIO for the management of that. Then the role of that Committee also is to facilitate the establishment of effective data governance and data-sharing capabilities across Government. I've been around a longish time as well and I see that we've made great strides in not just the integrity of our data, but our ability to utilise that for the benefit of Tasmanians but also to share that as well.

This is obviously a journey. We are an old organisation, being a Government, there's lots of legacy systems and processes, but I think the focus on that is important, moves us towards a digital Government scenario which is really where we want to get to. Then just finally that Committee does report to the Secretaries' Board on a monthly basis, so it then goes up the line and - sorry Chair, just one thing reflecting on your comments around telecommunications, again, very complex sector and market, Federal Government obligations, private sector and also State Government as a customer.

I, as the Digital Minister also sit on the Federal Digital and Data Ministers' meetings and you well be pleased to know I am very much a squeaky wheel in relation to Tasmania getting a fair go when it comes to communications telco. Particularly from the Federal Government perspective and their investment, which I think has been a bit sluggish, but we're keeping the pressure on. Thank you.

***CHAIR** - ... You do say you've adopted this in principle but it seems pretty much that you've adopted it, is there an explanation for that?*

...

***Ms KELLY** - I'm not quite sure why it was marked as in-principle because it was adopted in - we've been running since 2022 and it's a really productive group. In terms of reporting to the secretary's board - we do meet monthly, we met this morning for example, for two hours and we actually - and Justin mentioned before there's a standing meeting held every week which is to talk more operational and the idea of the DSC meetings, monthly, is to deal with those strategic issues.*

Besides providing a report to the Secretaries' Board - and the Secretaries' Board sign off on our annual work plan - besides providing written reports every month there is also the opportunity to go and meet with the secretaries' board and address any questions that they might have either about our papers or about the direction that we're taking.

***CHAIR** - We can say that one has been accepted?*

***Ms KELLY** - I would say accepted and completed and ongoing -*

...

***Dr THURLEY** - I can answer why it's like that -*

...

***Dr THURLEY** - In 2020 when it was on the table, there was the response back from Government and it's in the front matter of the report - was like, 'Oh, we're not sure about what you're asking here, we want to have a think about it and reform it, potentially in a different way,' and the reform is actually very different than what the Auditor asked for, but it's better and it's more modern, and, over the next three years we've just - that's where it's adopted to. We've ended up in a place that's better and fully adopted what he was after in intent.*

***CHAIR** - Yeah that's what I'm saying, just achieved it in a slightly different way.*

***Dr THURLEY** - Yeah, that's right.*[22]

Committee Findings

F8. The Government has reviewed the terms of reference for the Digital Services Board and it is reviewed annually.

---

[22] See Public Hearing (5 February 2026) - Min Ogilvie, p.15-16

Auditor-General Recommendation 4

The Digital Services Board to review implementation of the whole-of-Government ICT strategy to ensure it supports the Government's ICT vision and ensure plans are developed to implement the strategy.

DPAC reported to the Committee it had accepted the Auditor-General's recommendation in full.[23]

DPAC provided the following as evidence of implementation or progress (continuous delivery):

> *The Data and Digital Subcommittee continue to meet on a monthly basis and provide a monthly report on activities underway to the Secretaries Board.*
>
> *An annual workplan is submitted to the Secretaries Board for endorsement.*
>
> *The Data and Digital Subcommittee has regular*[ly] *reviewed progress against the Our Digital Future Strategic Action Plan.*

DPAC relied upon Attachments D, J and K as supporting evidence for this recommendation.

At the public hearing, Minister Ogilvie, Dr Thurley and Ms Kelly provided the following:

> ***Ms OGILVIE** - I would just very briefly say that I think a power of work has been done and yes, adopted, but it's always a question of how to make sure in adopting recommendations we fit them and the process we adopt is best practice and best process. I think that's really how we've gone about it. A great credit to everybody who did the original work and also the journey to get to this point in time, it's not perfect, but I think we're shaping things up well.*
>
> ***CHAIR** - ... We've talked about this in how the Board operates and the annual work plan which you provide a copy of the 2025 work plan in the documentation provided: in the current budgetary constraint environment we're in, will the prioritisation of these projects need to be reconsidered, and how will you go about that as the Minister?*
>
> ***Ms OGILVIE** - As the Minister, I will always advocate for more and better investment in technology right across Government, but I will note that a number of our projects are not subject to this particular budget cycle, they run across a number of budget cycles.*
>
> *I think we are a very efficient and effective group. It is, in fact, our CIO who has his finger on the pulse of that. I will say I have not heard of any desire to start cutting projects, I think that would be concerning, but we do have a need, I think, to really make sure that what we're doing from an investment in the IT projects perspective is really well-targeted - and I know we like to talk about the stack - but it is addressing the foundational systems work that we need to do right across Government, and allowing space to do innovative and agile things as well. We're starting to see a few of those*

[23] See Attachment A, p.6

happen. The reason we can do that is because we have this new governance model in place where we're actually connecting people in a smarter way.

I think that that's my top level response. I wonder, Justin, whether you might just talk more broadly to how prioritisation in decision-making for IT investment generally happens. ...

***Dr THURLEY** - ... Particularly at the whole-of-Government level - and I won't speak for each agency because their prioritisation will be based on their risks and requirements and opportunities, strategic risks and opportunities, would be the way I'd phrase that - but for the whole-of-Government, we look at where we can make the biggest impacts with the work that we've identified in our work plan, because we often have more than we can do in our work plan, and often our work plan is quite elaborate.*

We just went through a process today where we changed it again, to see if we can just focus on things where we can make a difference, and also try and focus on Government's priorities. We try and identify what priorities Government is telling us it has. We then work our way down through what the business priorities are and then into the work that we are doing to make sure that we are aligning with the Government's priorities.

We look at things like cost optimisation, or we're looking at improving a particular digital service's delivery like we did with My Service Tas, or we're looking at improving cybersecurity, and we have a number of projects still in that space. Similarly, the digital workplace and capability - or digital workforce and capabilities - are still something that we'd like to move forward with where we can.

All those different areas that operate in, we try to tie them back to the Government's priorities of the day, and make sure that we are continuously aligned with it. We will review it, make sure it's the thing that we're getting the best bang for our buck out of, and ensure that we are doing the right projects, that they're for the whole-of-Government. Each inner agency goes through a similar process, and again, I'd say it's more focused on the strategic opportunities and risks.

***Ms KELLY** - ... we do that collectively through the Data and Digital Committee. In developing our work plan that we were finalising today, we spent a couple of meetings last year talking as a Committee about, at a whole-of-Government level, what are the priorities? What are the priorities that are at an agency level as well? We used different tools and things like that to prioritise and work through what was going to be number one through to ten.*

We also have different streams of work. Some of the work that we do, some of the initiatives we might have on our work plan, are things that we're going to oversee that we've got an interest in, but we're not necessarily doing the work, it lives with a particular agency or business area. There are some things on our work plan that we're going to investigate.

An example of that which ties into one of the first questions we were talking through is, is it beneficial to Government to have one desktop platform, so everyone has one device or

a variety of the device, across the whole of the State service? Therefore, do you then have one IT help desk and desktop support team to manage that across Government? We're doing some work - and actually, DECYP are leading that work at the moment, around looking at the costs and the benefits of that so that we can then, depending on what we find, put up a proposal through to the Secretaries to say, look, we think there's something here. We think there's cost benefits to Government, we think there's efficiency benefits - would you like us to proceed?

The work plan will be made up of different categories of activities that the DDC have responsibility for and some of them are enduring as well, so they will span across multiple years. There are very few things that we put in our work plan that begin in January and end in December: usually they last through multiple years.

***Mr JAENSCH** - Surely there are organisations bigger than our whole public service that put out a tender to say 'set us up with our systems' routinely, all over the world. How are we still having to diagnose whether it's a good idea to be having one system or many? ...*

***Dr THURLEY** - It's a really good question because we do that sort of thing already. If you look at the ... function or the IT function on the digital platforms, et cetera, it's actually a complex area. To get one organisation to do all of it would be complicated and highly risky, I suspect. Not to say that it's not possible, and it does happen in big organisations -*

***Mr JAENSCH** - I'm not just necessarily suggesting getting an organisation in to do it, but maybe even being that organisation. Are we still working out if that's a good idea or not, to have a single integrated system?*

***Dr THURLEY** - ... I think we kind of are still working that out because of the nature of the autonomy and risk that you have within the way the Government is structured. If you wanted to just run it all out of a central agency, or a central entity, then it's absolutely possible, and that is done elsewhere. You'd have to look at the economics of it and we would have to look at that to see where it is.*

... If we're purely about cost optimisation, then that might be still the best way forward, but if we do need the autonomy to move things around, then we'd probably look at some sort of hybrid version of it, which is what most companies do...[24]

Committee Findings

F9. Through the Digital Services Board, the Government has provided plans and is continuously reviewing the implementation of the whole-of-Government ICT vision and strategy: this work is ongoing.

[24] See Public Hearing (5 February 2026) - Min Ogilvie, p.16-19

Auditor-General Recommendation 5

Agencies proactively plan and prioritise long-term, large scale and high value key ICT asset investment more effectively by improving their understanding of their current ICT environments and collaborating where mutual benefits exist.

DPAC reported to the Committee it had accepted the Auditor-General's recommendation in principle:[25]

> *Future agency planning and prioritisation of investment in key ICT assets will be informed by the strategic action under Our Digital Future to develop a whole-of-Government Technology Roadmap.*
>
> *Agencies consider that this recommendation does not recognise* [the] *diverse nature of their respective business and portfolio drivers – including, for some, interactions with national systems - and rapid changes in the technology sector.*

DPAC provided the following as evidence of implementation or progress (continuous delivery):

> *Our Digital Future – Strategic Action Plan was first published in 2020 and is reviewed annually.*
>
> *Agencies are also committed to developing long term plans.*
>
> *Since finalisation of the ICT Strategy, Critical Systems and Investment Audit Report Agencies have progressed the renewal or replacement of a considerable number of ICT systems and assets through various programs and plans. This is evidenced in budget papers from 2020-21 through to 2024-25.*
>
> *Examples include:*
>
> - *Tasmanian Government Radio Network (TASGRN) – TASGRN went live in July 2024 providing a single, unified, and secure digital radio network for emergency services and other government users across Tasmania.*
> - *Networking Tasmania – The government's private interagency network connecting government has seen uplift and renewal through continued investment and planning.*
> - *The Digital Communications Transformation – In 2021 Digital Strategy and Services within the Department of Premier and Cabinet commenced a program to explore the future state of whole-of-Government digital communications.*
> - *Fisheries Digital Transition Project - Transitioning Tasmania's commercial wild-capture fisheries to digital processes, including the FishPort web portal and FishReport mobile application.*
> - *PlanBuild Tasmania Portal - Streamlining the process for lodging and assessing planning, building, and other applications to local councils.*

[25] See Attachment A, p.7

- *myServiceTas Digital Services Portal - Developing a secure, easy-to-use access point for government services, including driver licence renewals and vehicle registration.*
- *Digital Health Transformation – The Tasmanian Government's Digital Health Transformation Program (2022-2032) is a 10-year, $476 million initiative being delivered by the Department of Health that focuses on leveraging digital technologies to improve patient outcomes by creating a more connected and accessible health system for all Tasmanians.*
- *Project Unify – Project Unify is an initiative being delivered by the Department of Police, Fire and Emergency Management and is focused on upgrading outdated ICT systems within Tasmania Police to enhance operational efficiency, data security, and information access for frontline officers.*
- *Justice Connect – Justice Connect is a project within the Department of Justice that focused on a major digital transformation of the state's justice system, aiming to replace outdated systems with an integrated end-to-end digital solution called Astria. This is being implemented in stages; the initial focus is on criminal and corrective justice.*
- *eCabinet – The eCabinet project delivered by the Department of Premier and Cabinet has successfully delivered a modern electronic workflow system to streamline Cabinet processes for the Cabinet Office, Ministers' Offices, and government departments, aiming for improved efficiency in handling Cabinet documents and decisions.*

DPAC relied upon Attachments C to G and I, and Tasmanian Budget Papers 2020-21 to 2024-25[26] as supporting evidence for this recommendation.

At the public hearing, Dr Thurley provided the following:

> ***CHAIR*** *- ... With Recommendation 5, and this, again, is one accepted in principle. I just note that the implementation progress has, since finalisation of the ICT strategy, critical systems and investment audit report agency progressed with renewal and replacement of considerable number of ICT systems and assets through various programs and plans, and that's outlined in the budget papers from 2020-21 to the more recent budgets. You've provided some information, as you did previously, about some of the agencies that have done a lot of this work. Why is this one accepted in principle and what different alternative approaches have you taken?*
>
> ***Dr THURLEY*** *- Again, I think the main reason this one was accepted in principle was the interconnectedness it has to Recommendations 1 through to 3, and for the same reasons, the Auditor's report was very specific about how it wanted ICT planning to happen. ... there was very much a different version of that being played out in State Government at the time and also in alignment with events at the time. I think it's more about the fact that we went for a more modern and contemporary approach than perhaps the traditional approach that was put into the report.*[27]

[26] See Department of Treasury and Finance, 'Budget Papers Archive'. Accessed at: https://www.treasury.tas.gov.au/budget-and-financial-management/2025-26-tasmanian-budget/budget-papers-archive

[27] See Public Hearing (5 February 2026) - Min Ogilvie, p.19-20

In relation to the different approach taken in the adoption of the Auditor-General's recommendation, the Committee noted that Ms Jenny Gale (then Secretary, DPAC and Secretary, Digital Services Board) in her response to the Auditor-General's Report stated:

> *Agencies consider the report does not recognise diverse nature of their respective business and portfolio drivers – including, for some, interactions with national systems - and rapid changes in the technology sector. Future agency planning and prioritisation of investment in key ICT assets will be informed by the strategic action under Our Digital Future to develop a whole-of-Government Technology Roadmap.*[28]

Committee Findings

F10. Whilst accepting the Auditor-General's recommendation in principle, the implementation of the whole-of-Government approach has taken a 'modern and contemporary approach' to ICT planning and investment by the Digital Services Board.

---

[28] See Report No. 4 of 2020-21 – Information and communications technology, critical systems and investment, https://www.audit.tas.gov.au/wp-content/uploads/ICT-Strategy-Report-Final-Report.pdf, p.9

Auditor-General Recommendation 6

The Department of Treasury and Finance revisit the feedback approach for Structured Infrastructure Investment Review Process (SIIRP) submissions to better inform agencies on areas for improvement for future SIIRP submissions.

DPAC reported to the Committee it had accepted the Auditor-General's recommendation in principle:[29]

> *Treasury had indicated through the findings that it considered SIIRP[30] process an effective process to evaluate investment proposals.*
>
> *As part of the DSB management response, the Department of Treasury and Finance agreed to review its feedback and guidance to agencies seeking funding through the SIIRP process rather than modify its approach to providing feedback.*

DPAC provided the following as evidence of implementation or progress (partially completed in October 2021):

> *Feedback was provided by Treasury suggesting ICT business cases developed from SIIRP often failed to articulate the benefits or provide accurate costs for ICT based investments.*
>
> *Treasury provided additional resources for Agencies to use as guidance: however, these resources did not directly address implementing a change in the approach for providing feedback.*
>
> *In 2023 DPAC Digital Strategy and Services initiated work to review the Treasury guidance and explore practices relating to ICT investment funding and assurance used in other jurisdictions. Additional funding and resourcing have not been identified to continue this work.*
>
> *Since October 2020, a range of ICT related proposals have been initiated via SIIRP, high profile examples being – the development of the strategy that unpins the Digital Transformation Program in Health, and the preliminary business case for Justice Connect.*

DPAC relied upon an 'increase in the number of successful SIIRP proposals following additional awareness and guidance work' as supporting evidence for this recommendation.

At the public hearing, Dr Thurley and Ms Kelly provided the following:

> ***CHAIR -*** *...You talked about this earlier, Minister, I think in your opening comment, to revisit the feedback approach to the SIIRP submissions to better inform agencies on areas for improvement on future SIIRP submissions. You say you've accepted that in principle, and you've talked about how you've changed some of that. How are you measuring the outcomes of this? Has it made a difference?*

[29] See Attachment A, p.9

[30] Structured Infrastructure Investment Review Process

...

***Dr THURLEY** - I'm happy to talk about that. SIIRP was a process that in the day, particularly around 2020, wasn't well understood by the agencies in terms of how they could use it to build out their projects. In particular, it derisks projects. For example, if someone comes in and asks for a big sum of money and then works out they can't deliver it or it's not right or I need more money - those sorts of things - trying to avoid that. Spending more time on the investment analysis and getting the options right to a level that Treasury can be satisfied that there has been some robust analysis done.*

A lot of work has gone on since then. Education, the uplift in our understanding and approach to how we get business cases done, how we do investment analysis for IT projects - there's a lot of work that's gone on and maturity that's occurred around if I want to get -

***CHAIR** - How's that work been done? What have you done to achieve that?*

***Dr THURLEY** - I think it's probably been more organic in the culture buildout, from 2020 through to now. We've hit the ground running with COVID. A lot changed in terms of how IT is perceived and the profile that it had. A lot of the time we were running with these projects that looked a little bit risky and a little bit uncertain. How do we then cover off on how we build good cases and good understandings of our projects, and also the ability to back out of a project when it's not going to work? This is where, I think, everybody's understanding, the maturity in the industry, the maturity in Government about understanding how to do investment for ICT, has really changed in those five years. Now, if I want to replace the motor registry system, for example, I would have to do a fairly robust business case to say, why should Government spend x millions of dollars, and be able to show that business case is being developed appropriately with some accurate and defendable numbers.*

***CHAIR** - That's operation normal now?*

***Dr THURLEY** - Yes, I think it is. I'm not thinking about getting an ICT project through Treasury or anything like that, that doesn't meet a very high standard of understanding what the risks are.*

***CHAIR** - You say that the supporting evidence - you just talked about it but didn't actually provide actual evidence - increase the number of successful SIIRP proposals. Have you got a metric on that?*

***Dr THURLEY** - Yes. Which projects were born out of SIIRP would be the way I'd do that. If you were going to say how many projects it would be, it would be less than a dozen over the years in ICT. There's lots of other projects we go through, but we do know that from 2020 when there was none, we've had several that have gone through that process. Particular ones would be the Digital Health Transformation that started in that space, and Justice Connect, I believe, started in that place. We've also had other projects that have gone through SIIRP that may not have actually resulted in investments, which I won't go into.*

CHAIR *- Yes, which is the purpose of the process.*

Dr THURLEY *- Yes, correct, successful.*

Ms KELLY *- It also gives the opportunity to highlight to Treasury through the SIIRP process those systems that are potentially at risk as well, so rather than an agency necessarily just putting in a bid through to the annual budget submission process, there's that opportunity to build that case about why it's a risk and the consequences of not investing, so it can provide a parallel pathway.*[31]

Committee Findings

F11. Improved guidance on how to engage with the Structured Infrastructure Investment Review Process has occurred with a positive outcome.

F12. In 2023 DPAC Digital Strategy and Services initiated work to review the Treasury guidance and explore practices relating to ICT investment funding and assurance used in other jurisdictions: this work has not been completed.

---

[31] See Public Hearing (5 February 2026) - Min Ogilvie, p.20-21

Auditor-General Recommendation 7

Agencies maintain up-to-date ICT critical asset registers in a consistent format which identify key risks replacement dates and level of funding required.

DPAC reported to the Committee it had accepted the Auditor-General's recommendation in full:[32]

> *Agencies agreed to explore opportunities to build more consistent asset management practices.*

DPAC provided the following as evidence of implementation or progress (continuous delivery):

> *Agencies initiated various projects and activities to improve information and risks associated ICT critical asset*[s].
>
> *All agencies currently maintain a register of critical ICT assets, although there are differences across agencies that reflect the prioritisation of systems in terms of operational dependencies and the agencies* [sic] *appetite for risk.*
>
> *In 2024 the Department of Health initiated a program to enhance its ICT asset register by mapping the interlinked asset dependencies for the agency. The Data and Digital Committee resolved that this approach and the platform being used to accomplish the capability could be utilised by all agencies to enhance visibility of critical assets and assist to manage investment lifecycles. The committee agreed to add a project to 2025 Data and Digital Committee Work Plan to explore the establishment of a whole-of-Government critical systems register, with a view to extend the register into an investment planning.*
>
> *The DDC's role in defining the methodology for asset management and format of registers will also be captured in the Terms of Reference.*
>
> *The Tasmanian Government has further strengthened the requirements for managing critical ICT assets with the development and implementation of the Tasmanian Protective Security Policy Framework (PSPF). Specifically, INFOSEC-3 requires that Accountable Authorities ensure the security of technology and information assets to safeguard data, information and privacy, and to ensure continuous delivery of government business during all stages of the asset life cycle.*

DPAC relied upon Attachments D, L, and PSPF INFOSEC-3[33] as supporting evidence for this recommendation.

At the public hearing, Minister Ogilvie, and Dr Thurley provided the following:

[32] See Attachment A, p.10

[33] See Tasmanian Government, 'INFOSEC-3: Robust technology and information systems'. Accessed at: https://www.security.tas.gov.au/protective-security/information-security/infosec-3-robust-technology-and-information-systems

CHAIR *- Recommendation 7 is about the up-to-date ICT critical asset registers. Have all agencies now got them?*

Dr THURLEY *- Up-to-date ICT asset registers? Yes, to my knowledge. You know, I'm not going to pull one out and say it's up to date as of today, but yes.*
...
Ms OGILVIE *- ... My reflection is we've come a long way since that report, and I'd like to thank the department for the work that they're doing. It's obviously an iterative process and turning legacy systems and processes into a modern Government digital system is challenging, but I think we're up to the challenge, given budgetary constraints as well.*

There's lots of really interesting things happening and I think our workforce is quite sophisticated and digitally switched on and we intend to invest time and energy in making sure we maintain that - and of course, we're interested in the broader Tasmanian perspective as well.[34]

Further advice with respect to the consistency of ICT critical asset registers across agencies was received from Ms Noelene Kelly (Deputy Secretary, DPAC):

While agencies share a common understanding of what constitutes a critical ICT asset, the form, structure and level of detail of these registers are not yet fully consistent across Government. Differences reflect agency autonomy, operational context, system complexity and risk appetite.[35]

Committee Findings

F13. In 2024 the Department of Health initiated a program to enhance its ICT asset register by mapping the interlinked asset dependencies for the agency.

F14. The Data and Digital Committee resolved that Department of Health approach and the platform being used to accomplish the capability could be utilised by all agencies to enhance visibility of critical assets and assist to manage investment lifecycles.

F15. All agencies now have up-to-date ICT critical assets register. It is not clear whether they are of a consistent form.

F16. The Data and Digital Committee agreed to add a project to 2025 Data and Digital Committee Work Plan to explore the establishment of a whole-of-Government critical systems register, with a view to extend the register into an investment planning.

[34] See Public Hearing (5 February 2026) - Min Ogilvie, p.21
[35] Email to Committee, Ms Noelene Kelly (Deputy Secretary, Community and Government Services) DPAC dated 20 March 2026

Committee Recommendations

R3. As supported by the Data and Digital Committee, all agency ICT critical asset registers be consistent with the Department of Health template approach to mapping the interlinked asset dependencies.

R4. The Data and Digital Committee continue to explore the establishment of a whole-of-Government critical systems register.

Summary of Attachments

Attachment A	Letter from Shane Gregory (Associate Secretary, DPAC) to Committee dated 28 July 2025
Attachment B	Our Digital Future: Tasmanian Government strategy for digital transformation
Attachment C	Our Digital Future: Strategic Action Plan
Attachment D	Data and Digital Subcommittee Work Plan 2025
Attachment E	DoJ ICT Strategy 2017 – 2022
Attachment F	DNRET Digital and Data Services Strategic Roadmap 2024 – 2027
Attachment G	DECYP IT Infrastructure Plan 2024 – 2029
Attachment H	DSS Roadmaps 2022
Attachment I	DSS Roadmap Networks and Infrastructure 2022
Attachment J	Data and Digital Committee Terms of Reference
Attachment K	Example Progress Tracking – Our Digital Future Strategic Action Plan
Attachment L	Example Data Dictionary for the NRE Information Asset Register

Department of Premier and Cabinet

Executive Building 15 Murray Street HOBART TAS 7000 Australia
GPO Box 123 HOBART TAS 7001 Australia
Ph: 1300 135 513 Fax: (03) 6233 5685
Web: www.dpac.tas.gov.au

Tasmanian Government

Hon Ruth Forrest MLC
Chair
Parliamentary Standing Committee of Public Accounts
By email to: Simon.Scott@parliament.tas.gov.au

Dear Ms Forrest

Re. Follow-up of Auditor-General Report No.4 of 2020-21 – Information and Communications Technology Strategy, Critical Systems and Investment and Response to the Public Accounts Committee Questionnaire

With reference to your correspondence to the Minister for Innovation, Science, and the Digital Economy dated 29 May 2025, I write to provide a response to the Committee's questions regarding the extent to which the recommendations of the *Auditor-General Report No.4 of 2020-21 – Information and Communications Technology Strategy, Critical Systems and Investment* (ICT Strategy, Critical Systems and Investment Audit) have been implemented by Government.

Work relating to the ICT Strategy, Critical Systems and Investment Audit commenced in 2019 with the final report being published in August 2020. As this audit was progressing two initiatives were underway that were also significant for digital and ICT in government – the *Tasmanian State Service Review* and the development of *Our Digital Future*. Further complicating matters, all three activities occurred during the COVID-19 pandemic.

The convergence of the Audit with the other three activities heavily influenced Government's response to the Audit recommendations, which are well summarised in the report's Executive Summary under the heading of "Collective response from Digital Services Board members" (pp8).

The Government's experience of the COVID-19 pandemic and its impact on Tasmanians reinforced the need for government to focus on digital services; to understand user needs and design and deliver accessible 'anytime, anywhere' services to protect Tasmanians and strengthen our economic recovery.

As a consequence, some of the recommended actions from the ICT Strategy, Critical Systems and Investment Audit were absorbed by *Our Digital Future* and the associated strategic action plan, and the digital reforms recommended in in the final report of the *Tasmanian State Service Review*. In fact, the recommendations of the ICT Strategy, Critical Systems and Investment Audit were referenced as informing the recommendations Tasmanian State Service Review.

Our Digital Future has been instrumental in driving a range of strategic digital and ICT investments that have delivered tangible benefits to the Tasmanian community. These achievements demonstrate the government's commitment to its digital transformation agenda and its ability to translate strategy into action.

The ongoing contribution of the Data and Digital Subcommittee, which was established via recommendations 24 and 25 of the *Tasmanian State Service Review,* also remains central to digital governance. Replacing the Digital Services Board as a standing subcommittee of the Secretaries Board, the Data and Digital Subcommittee provides continuous oversight of whole-of-government digital priorities, facilitates cross-agency coordination, and supports consistent data governance and information-sharing practices.

In addition to the whole-of-government impacts, agencies have also actively progressed digital transformation initiatives aligned with core business priorities. The collective momentum of these efforts, illustrate the diverse ways in which Government has adopted new digital and ICT technologies to improve operations and service delivery.

In relation to the recommendations from the *ICT Strategy, Critical Systems and Investment Audit*, and the questionnaire provided by the Public Accounts Committee, I have attached our response to the Committee's questionnaire. It outlines the key information relevant to the recommendations.

Your sincerely

Shane Gregory
Associate Secretary

28 July 2025

Enc: Response to Public Accounts Committee Questionnaire

Response to the Public Accounts Committee Questionnaire

Recommendation 1: The Government enhance ICT investment evaluation and prioritisation by developing, through its current ICT framework, a whole-of-government ICT vision informed by an understanding of each agencies key ICT assets, their age profile, key risks, interdepartmental reliance and proposed replacement timetable. This vision, and the strategy to implement it, should be developed as a priority. It should be delivered and executed within the next 18 months.

Acceptance	Implementation Progress	Supporting Evidence
Accepted in principle. • The Digital Services Board audit response, published in the final report outlined the boards position in relation to work that was already underway developing the Government's Digital Strategy, *Our Digital Future*. • The Board accepted the recommendation in principle but tempered the proposed response, indicating that "it would be inappropriate for the Government to define an ICT strategy or vision in the absence of a digital vision and strategy", and that *Our Digital Future* specifies the development of a whole-of-government technology roadmap as a strategic action and this body of work would address Recommendations 1 and 2 of the Audit.	***Continuous delivery*** • *Our Digital Future* was released in June 2020 and this strategy set a broader strategic context for digital transformation and articulated the government's commitment to leveraging digital technologies to improve the lives of Tasmanians, drive economic growth, and enhance public service delivery. • Later in 2020 and also accounting for urgent actions required to support the COVID-19 recovery, Government release the *Strategic Action Plan* supporting *Our Digital Future*. • Under the digital government workstream, an action was included to develop a whole of government technology road map. • Critically the development of this roadmap for whole-of-government has been largely subsumed into the annual *Data and Digital Subcommittee Work Plan*, it is also recognised that the pragmatic development of detailed technology roadmaps is undertaken by system owners and those who deliver the systems working in alignment with government digital priorities, directions and standards (whole of government or within agencies).	• *Our Digital Future* https://www.digital.tas.gov.au/downloads/Our-Digital-Future.PDF • *Our Digital Future* – Strategic Action Plan https://www.digital.tas.gov.au/downloads/Our-Digital-Future-Strategic-Action-Plan.pdf • Attachment 1. Data and Digital Subcommittee Work Plan 2025. ..

Recommendation 2: The WoG ICT vison and strategy identify – (a) key priorities for the short, medium, and longer term; (b) strategies for greater collaboration targeting cost efficiency gains, increased productivity, removal of duplication of effort across agencies and alignment to government strategy and policy; (c) known key ICT assets targeted for replacement or renewal; and (d) critical assets that are significantly aged or at potential risk of failure.

Acceptance	Implementation Progress	Supporting Evidence
Accepted in principle. • As for Recommendation 1.	***Continuous delivery*** • Establishment of the Data and Digital Subcommittee of the Secretaries Board and its annual work program addresses planning for the short-, medium- and longer-term whole-of-government initiatives that are focused on collaboration, efficiencies and policy alignment. • The 2024 and 2025 work programs have comprised five active work streams – Digital Services, Common Systems and Platforms, Data and Information Governance, Cyber Resilience and Risk, and Digital Workforce Capabilities. • Agency ICT strategies and infrastructure plans address plans for assets primarily supporting agency outputs, although there are exceptions for shared capabilities and service across various agencies. • Whole of government digital infrastructure and common business systems are predominantly delivered by DPAC Digital Strategy and Services (DSS). DSS maintains detailed roadmaps and plans for those services. • Similarly, addressing recommendations 5 and 7 has allowed agencies to progress the replacement and renewal of ICT assets and to help identify critical assets that are significantly aged or at potential risk of failure (see responses outlined for recommendation 5 and 7).	• *Our Digital Future* https://www.digital.tas.gov.au/downloads/Our-Digital-Future.PDF • *Our Digital Future* – Strategic Action Plan https://www.digital.tas.gov.au/downloads/Our-Digital-Future-Strategic-Action-Plan.pdf Selected example strategies, roadmaps and plans: • Attachment 1. Data and Digital Subcommittee Work Plan 2025 • Attachment 2. Department of Justice (DoJ) ICT Strategy 2017 -2022 • Attachment 3. Department of Natural Resources and Environment Tasmania (NRE) Digital & Data Services Strategic Roadmap 2024 – 2027 • Attachment 4. Department for Education, Children and Young People (DECYP) IT Infrastructure Plan 2024 to 2029 • Attachment 5. Digital Strategy and Services Whole of Government Services Roadmaps 2022 • Attachment 6 - DSS Roadmap Networks and Infrastructure 2022

Recommendation 3: The government review the terms of reference for the Digital Services Board (DSB) to ensure it has the mandate to better support a prioritised and collaborative approach to ICT across agencies with DSB providing support and guidance, where needed, to agencies for ICT strategic planning and management of critical asset.

Acceptance	Implementation Progress	Supporting Evidence

Accepted in principle.
 	
• In its audit response the DSB advised that if a formal review of ICT governance was to be undertaken, it should be an end to end review and include the entire ICT governance framework including the Terms of Reference for both the Deputy Secretaries Digital Services Committee (DSDSC) and the role of the Digital Services Advisory Group (DSAG), noting that a biennial review was already part of the Terms of Reference of each of these governance bodies.
	Completed April 2022
	
	• The ICT Governance Framework was subsequently reviewed and restructured in response to recommendations 24 and 25 of the Tasmanian State Service Review.
	
	• In April 2022, the newly formed Tasmanian Government Secretaries Board established the Data and Digital Sub-committee comprising agency CIOs and key information management stakeholders from across government.
	
	• The endorsed role of the Data and Digital Subcommittee is to:
	
	  ○ oversee whole-of-government digital initiatives;
	
	  ○ monitor progress and the delivery of significant government digital priorities (including Our Digital Future);
	
	  ○ lead engagement and collaboration across government agencies to promote a user-focused, and 'one government' approach to the design and delivery of digital services; and
	
	  ○ facilitate the establishment of effective data governance and data sharing capabilities across government.
	
	• The Terms of Reference are reviewed on an annual basis.
		• Recommendations 24 and 25 in the Tasmanian State Service Review pp134 https://www.dpac.tas.gov.au/divisions/policy/review_of_the_tasmanian_state_service/TSSR_Final_Report.pdf
		
		• Attachment 7. Data and Digital Committee Terms of Reference.

Recommendation 4: The DSB to review implementation of the WoG ICT strategy to ensure it supports the government's ICT vision and ensure plans are developed to implement the strategy.

Acceptance	Implementation Progress	Supporting Evidence
Accepted in full	***Continuous delivery*** • The Data and Digital Subcommittee continue to meet on a monthly basis and provide a monthly report on activities underway to the Secretaries Board. • An annual workplan is submitted to the Secretaries Board for endorsement. • The Data and Digital Subcommittee has regular reviewed progress against the *Our Digital Future Strategic Action Plan.*	• Attachment 7. Data and Digital Committee Terms of Reference, and endorsed role to monitor progress and the delivery of significant government digital priorities (including Our Digital Future); • Attachment 1. Data and Digital Subcommittee Work Plan 2025. • Attachment 8. example progress tracking for the *Our Digital Future Strategic Action Plan.*

Recommendation 5: Agencies proactively plan and prioritise long-term, large scale and high value key ICT asset investment more effectively by improving their understanding of their current ICT environments and collaborating where mutual benefits exist.

Acceptance	Implementation Progress	Supporting Evidence
Accepted in principle. • Future agency planning and prioritisation of investment in key ICT assets will be informed by the strategic action under Our Digital Future to develop a whole-of-government Technology Roadmap. • Agencies consider that this recommendation does not recognise diverse nature of their respective business and portfolio drivers – including, for some, interactions with national systems - and rapid changes in the technology sector.	***Continuous delivery*** • Our Digital Future – Strategic Action Plan was first published in 2020 and is reviewed annually. • Agencies are also committed to developing long term plans. • Since finalisation of the ICT Strategy, Critical Systems and Investment Audit Report Agencies have progressed the renewal or replacement of a considerable number of ICT systems and assets through various programs and plans. This is evidenced in budget papers from 2020-21 through to 2024-25. Examples include: • Tasmanian Government Radio Network (TASGRN) – TASGRN went live in July 2024 providing a single, unified, and secure digital radio network for emergency services and other government users across Tasmania. • Networking Tasmania – The government's private interagency network connecting government has seen uplift and renewal through continued investment and planning. • The Digital Communications Transformation – In 2021 Digital Strategy and Services within the Department of Premier and Cabinet commenced a program to explore the future state of whole-of-government digital communications. • Fisheries Digital Transition Project - Transitioning Tasmania's commercial wild-capture fisheries to digital processes, including the FishPort web portal and FishReport mobile application.	• *Our Digital Future* – Strategic Action Plan https://www.digital.tas.gov.au/downloads/Our-Digital-Future-Strategic-Action-Plan.pdf • Budget Papers 2020-21 through 2024-25 https://www.treasury.tas.gov.au/budget-and-financial-management/2025-26-tasmanian-budget/budget-papers-archive Selected example plans from agencies: • Attachment 1. Data and Digital Subcommittee Work Plan 2025 • Attachment 2. DOJ ICT Strategy 2017 -2022 • Attachment 3. NRE Digital & Data Services Strategic Roadmap 2024 – 2027 • Attachment 4. DECYP IT Infrastructure Plan 2024 to 2029 • Attachment 6 - DSS Roadmap Networks and Infrastructure 2022

	• PlanBuild Tasmania Portal - Streamlining the process for lodging and assessing planning, building, and other applications to local councils. • myServiceTas Digital Services Portal - Developing a secure, easy-to-use access point for government services, including driver licence renewals and vehicle registration. • Digital Health Transformation – The Tasmanian Government's Digital Health Transformation Program (2022-2032) is a 10-year, $476 million initiative being delivered by the Department of Health that focuses on leveraging digital technologies to improve patient outcomes by creating a more connected and accessible health system for all Tasmanians. • Project Unify – Project Unify is an initiative being delivered by the Department of Police, Fire and Emergency Management and is focused on upgrading outdated ICT systems within Tasmania Police to enhance operational efficiency, data security, and information access for frontline officers. • Justice Connect – Justice Connect is a project within the Department of Justice that focused on a major digital transformation of the state's justice system, aiming to replace outdated systems with an integrated end-to-end digital solution called Astria. This is being implemented in stages; the initial focus is on criminal and corrective justice. • eCabinet – The eCabinet project delivered by the Department of Premier and Cabinet has successfully delivered a modern electronic workflow system to streamline Cabinet processes for the Cabinet Office, Ministers' Offices, and government departments, aiming for improved efficiency in handling Cabinet documents and decisions.	

Recommendation 6: Treasury to revisit the feedback approach for SIIRP submissions to better inform agencies on areas for improvement for future SIIRP submissions.

Acceptance	Implementation Progress	Supporting Evidence
Accepted in principle. • Treasury had indicated through the findings that it considered SIIRP process an effective process to evaluate investment proposals. • As part of the DSB management response, the Department of Treasury and Finance agreed to review its feedback and guidance to agencies seeking funding through the SIIRP process rather than modify its approach to providing feedback.	***Partially completed October 2021*** • Feedback was provided by Treasury suggesting ICT business cases developed from SIIRP often failed to articulate the benefits or provide accurate costs for ICT based investments. • Treasury provided additional resources for Agencies to use as guidance; however, these resources did not directly address implementing a change in the approach for providing feedback. • In 2023 DPAC Digital Strategy and Services initiated work to review the Treasury guidance and explore practices relating to ICT investment funding and assurance used in other jurisdictions. Additional funding and resourcing have not been identified to continue this work. • Since October 2020, a range of ICT related proposals have been initiated via SIIRP, high profile examples being – the development of the strategy that unpins the Digital Transformation Program in Health, and the preliminary business case for Justice Connect.	• Increase in the number of successful SIIRP proposals following additional awareness and guidance work.

Recommendation 7 Agencies maintain up-to-date ICT critical asset registers in a consistent format which identify key risks replacement dates and level of funding required.

Acceptance	Implementation Progress	Supporting Evidence
Accepted in full. • Agencies agreed to explore opportunities to build more consistent asset management practices.	***Continuous delivery*** • Agencies initiated various projects and activities to improve information and risks associated ICT critical asset. • All agencies currently maintain a register of critical ICT assets, although there are differences across agencies that reflect the prioritisation of systems in terms of operational dependencies and the agencies appetite for risk. • In 2024 the Department of Health initiated a program to enhance its ICT asset register by mapping the interlinked asset dependencies for the agency. The Data and Digital Committee resolved that this approach and the platform being used to accomplish the capability could be utilised by all agencies to enhance visibility of critical assets and assist to manage investment lifecycles. The committee agreed to add a project to 2025 Data and Digital Committee Work Plan to explore the establishment of a whole of government critical systems register, with a view to extend the register into an investment planning. • The DDC's role in defining the methodology for asset management and format of registers will also be captured in the Terms of Reference. • The Tasmanian Government has further strengthened the requirements for managing critical ICT assets with the development and implementation of the Tasmanian Protective Security Policy Framework (PSPF). Specifically, INFOSEC-3 requires that Accountable Authorities ensure the security of technology and information assets to safeguard data, information and privacy, and to ensure continuous delivery of government business during all stages of the asset life cycle.	• Attachment 1 Data and Digital Subcommittee Work Plan 2025, pp6 (item 25/02 Critical Systems and Infrastructure Investment Plan Initiative). • Attachment 9. Example Data Dictionary for the NRE Information Asset Register. • PSPF INFOSEC-3 https://www.security.tas.gov.au/protective-security/information-security/infosec-3-robust-technology-and-information-systems

Supporting Attachments:

Attachment	Title
1	Data and Digital Subcommittee Work Plan 2025, pp6
2	DOJ ICT Strategy 2017 -2022
3	NRE Digital & Data Services Strategic Roadmap 2024 – 2027
4	DECYP IT Infrastructure Plan 2024 to 2029
5	Digital Strategy and Services Whole of Government Services Roadmaps 2022
6	DSS Roadmap Networks and Infrastructure 2022
7	Endorsed Terms of Reference - Data and Digital Committee - March 2024
8	Example progress tracking for the *Our Digital Future Strategic Action Plan.*
9	Example Data Dictionary for the NRE Information Asset Register.

Attachment B

OUR DIGITAL FUTURE

Tasmanian Government strategy for digital transformation

MARCH 2020

Tasmanian Government

Digital Strategy and Services
Department of Premier and Cabinet
GPO Box 123
Hobart TAS 7001
Email: digital@dpac.tas.gov.au
Web: www.digital.tas.gov.au

CONTENTS

MESSAGE FROM THE MINISTER

The indisputable truth of modern life is that we are more mobile, more connected and more reliant on technology than ever before.

While our local and global communities may be geographically, socially, culturally and economically diverse, we are united by a common need: to interact with one another and transact business in an increasingly digital environment.

We must keep pace with this changing paradigm and seize the enormous opportunities before us. We must work to ensure that our communities, businesses, industries and public services are equipped to optimise the use and benefits of new technologies.

We must also safeguard the integrity of the digital data we use, share and manage on behalf of the people of Tasmania, using the information we derive from this data to develop more targeted and effective policies, supported by contemporary services that meet the needs of all Tasmanians.

The Government has been working hard to develop stronger, more productive linkages with business, industry, academia and the community. Our digital future relies heavily on the cooperative achievements of all sectors working together. For example, pursuing the opportunity for Tasmania to develop as a centre of academic and professional digital excellence, capable of attracting, mobilising and retaining a specialist workforce that is able to meet increasing local, national and international demand across core technology occupations.

We are also committed to enhancing existing and new collaborative partnerships to help improve the digital skills of people and businesses in our communities, and to providing more opportunities for digitally disadvantaged Tasmanians.

Our goal is to develop stronger foundations so that, in the future, more Tasmanians will be able to access and use 'anytime, anywhere' digital services and information. For the Government, that does not mean taking away our existing service options, such as face-to-face or phone access; it simply means developing an improved range of seamless services that offer more choice, greater convenience and flexibility.

In the years and decades to come Tasmania, like all jurisdictions, will continue to face social, environmental and economic challenges. The work we do now will help us to meet these challenges. Together, we can leverage the increasingly digital environment in which we all live and work, to achieve our personal best, improve the health and welfare of families and communities, and develop new skills and capabilities for our children, our businesses and our future.

I commend the vision and objectives of *Our Digital Future* and encourage you to work with us to turn our vision into reality, helping Tasmania to grow and flourish in the digital world.

Michael Ferguson MP
Minister for Science and Technology


Geoneon

STRATEGY AT A GLANCE

VISION

A prosperous and connected Tasmania, collaborating and thriving in a technology-enabled world

COMMUNITY	ECONOMY	GOVERNMENT
PRIORITIES		
Inclusion *Skills* *Engagement*	*Business* *Industry* *Workforce*	*Services* *Capability* *Infrastructure*
PRINCIPLES		
Accessibility *Ability* *Affordability*	*Capability* *Creativity* *Connectivity*	*Simplicity* *Security* *Strategy*
OBJECTIVES		
A more digitally engaged and confident community that is socially, culturally, economically and educationally connected People in urban and rural areas across all regions have greater opportunities to participate and interact online with local, national and global communities, businesses and information sources People are supported to engage with government in the way that suits them best People and businesses are able to interact with government in a simple, secure, streamlined and accessible digital environment	A sustainable, innovative and secure business community that welcomes and adopts emerging technologies, and is empowered to transact digitally in local, national and global markets A vibrant, interconnected and well-supported startup environment for digital entrepreneurs A talented, diverse and inclusive local workforce that values, attracts, trains and retains people with specialised technology skills Reliable, scalable, available and affordable digital communications infrastructure	Securely-managed government information and technology systems, able to support efficient, joined-up public services Evidence-led policy decisions enabled by authoritative, accessible and appropriately managed data Skilled and capable government staff, able to incorporate new digital approaches and support contemporary technology systems Government-provided services and business operations realise the benefits of cloud-based services

STRATEGY AT A GLANCE (CONTINUED)

COMMUNITY	ECONOMY	GOVERNMENT
MAJOR ACTIONS		
→ Deliver the Digital Ready for Daily Life program for digitally disadvantaged groups, including low income households, older Tasmanians and people not in paid employment → Strengthen opportunities for lifelong digital skills learning → Provide more options and opportunities for public access to 'anytime, anywhere' government services → Improve telecommunications infrastructure, particularly in rural and regional Tasmania → Increase 'smart city' technology to support urban communities and new technology businesses → Support transformative digital projects that improve the delivery of frontline services to Tasmanians	→ Empower local businesses through the Digital Ready for Business program → Work with industry, business and education partners to develop and promote digital education, career pathways and workforce capability → Accelerate technology startups and entrepreneurial pathways through targeted programs supported by the Office of the Coordinator-General → Build the export capabilities of technology businesses through the Tasmanian Trade Strategy 2019-2025 → Uplift the global branding of Tasmania's information technology industry → Work with industry providers to enhance the adequacy and reliability of Tasmania's digital communications infrastructure	→ Develop new frameworks for information management and data analytics → Develop a whole-of-government technology roadmap → Adopt a cloud-first policy approach across government agencies → Implement a cybersecurity program that prioritises critical asset protection across government → Develop digital culture and capability across government agencies → Streamline government processes for the procurement of technology services → Reduce government red tape through the adoption of digital solutions → Develop an agile, iterative and risk-managed approach to the management and delivery of digital projects and services

THE FUTURE IS NOW

Digital technologies have transformed the way we communicate, store and find information, deliver services and transact business.

People no longer expect to complete paper forms, wait in queues or provide the same information multiple times to the same organisation. People also expect to be able to interact quickly and efficiently with government in the way that suits them best, anywhere and anytime: over the counter, telephone or internet; at work, at home or on the move.

Digital transformation is often described as the fourth industrial revolution because of the revolutionary impact it has on human life and work, fusing technologies and blurring lines between physical, digital and biological spheres. The impact of digital transformation on businesses, industries and societies is far-reaching, not just in positive economic terms and job growth, but for environmental benefits as well.

Digital devices and sensors in the world around us connect, exchange data, interact and self-regulate. Agricultural sensors can monitor soil moisture and crop growth to automate watering. Smart city sensors can indicate when rubbish needs collecting and toilets need cleaning. Environmental resources can be better managed by matching supply with demand to minimise waste. The potential benefits of digital transformation are endless, but to realise these benefits Tasmania must develop new skills, capabilities and infrastructure.

Australia has one of the most connected populations in the world, embracing new digital devices and services with an enthusiasm that rivals other early adopting nations.[1] Tasmania contributes to, learns from and influences the Australia-wide digital transformation of government to meet the needs and expectations of citizens through active participation and collaboration in the work of the Australian Government's Digital Transformation Agency, the Australian Data and Digital Council and inter-jurisdictional committees and working groups across multiple portfolio areas.

Tasmania was the first Australian state to be connected to the National Broadband Network (NBN). Launceston is one of Australia's first smart cities, with city-wide networks that allow sensors in everyday objects to interact remotely to make life easier and improve the way systems work, such as controlling traffic and street lighting. Networks established in Launceston and other locations around the State provide ideal test platforms for entrepreneurs to create, trial and commercialise cutting-edge technology solutions.

In this technology-driven environment, Tasmanian businesses are increasingly adopting digital methods and tools to promote and deliver services and commercial transactions online. Our academic institutions, local research clusters, niche industries, stable workforce, world-renowned natural heritage and enviable lifestyle are capable of attracting, developing, sustaining and promoting Tasmania as a 'centre of digital excellence', encompassing education and training, exciting career opportunities and an appetite for innovative projects that contribute to better socioeconomic outcomes for the State and the nation.

Tasmanian people welcome the speed and convenience of services that simplify their personal and business interactions, at the same time expecting that information entrusted to government will be securely managed and appropriately shared across the relevant business areas of government agencies. For the Tasmanian Government, digital transformation offers opportunities to improve service quality, access equity and productivity, enabled by leveraging a combination of new approaches and technologies.

> ***Digital maturity is about adapting the organisation to compete effectively in an increasingly digital environment.***
>
> ***Maturity goes far beyond simply implementing new technology by aligning … strategy, workforce, culture, technology and structure to meet the digital expectations of customers, employees and partners.***
>
> ***Digital maturity is, therefore, a continuous and ongoing process of adaptation to a changing digital landscape.***[2]

1 EY Sweeney (2017) *Digital Australia: State of the Nation.*

2 Kane, Palmer, Nguyen Phillips, Kiron and Buckley (2017) *Achieving Digital Maturity.*

OUR DIGITAL MATURITY

Digital maturity can only be developed incrementally.

As the Tasmanian Government's first strategy for digital transformation, Our Digital Future articulates a strong commitment to helping and inspiring Tasmanian people, businesses, industries and government agencies through the initial, foundation-building phase.

Digital maturity means much more than embracing new technologies: it is an ongoing process of seeking out, adopting and encouraging new ways of doing things, challenging and changing conventional practices. It means innovating to remove unnecessary costs and activities. It means putting citizens at the heart of everything we do.

> ***Technology is important, but as an enabler, not an outcome.***

To transform into a digitally mature organisation, the Tasmanian Government must focus on building digital capability and innovation, leveraging new skills and emerging technologies to develop more responsive policies, reduce red tape and deliver better services.

Community service expectations cannot be met without keeping digital information and services secure and protected. Digital services cannot be delivered by an organisation that does not have the capability or skills it needs to innovate, source and support new technologies.

Our goal is to build the foundational infrastructure, partnerships and workforce capability necessary to facilitate digital transformation, while carefully managing and protecting the security and integrity of information and services.

The Government's progress towards digital maturity will be supported by the development of a whole-of-government technology roadmap that links planned initiatives with the objectives and priorities of *Our Digital Future*. The roadmap will be strengthened by robust governance and managed processes that allow for ongoing reprioritisation as new business needs, challenges and priorities emerge.

PRIORITY

OUR DIGITAL COMMUNITY

DIRECTION

All Tasmanians should have an equal opportunity to interact with digital services and information in ways that are easy to use, convenient and readily available.

The Tasmanian Government is committed to supporting initiatives that encourage the benefits of digital transformation to accrue more evenly across all sectors of the community and regions of the State. As more and more essential services and information sources are delivered online, people must be afforded equal access to the tools and skills necessary for them to successfully navigate the internet and participate freely in a digitally inclusive environment.

While Tasmania typically experiences lower levels of digital literacy and digital inclusion compared to mainland counterparts, these are improving. Tasmania's Department of State Growth is working collaboratively with industry partners, Libraries Tasmania, other government agencies and the Tasmanian community sector to develop targeted initiatives for lifelong learning and digital inclusion.

In pursuing a digital future, the Tasmanian Government's goal is to provide more responsive public services and information that can be easily understood and used by all Tasmanians, designed for access through mobile phones and other hand-held devices.

The success of this pursuit will largely depend upon delivering the right service in the right way, while continuing to provide alternative, more traditional options for people with different service preferences, different levels of ability and more complex needs.

Citizens interacting with government through secure 'anywhere, anytime' digital services can benefit from savings in time, effort and out-of-pocket travel costs for over-the-counter services, ultimately leading to more equitable and inclusive service delivery outcomes.

PRINCIPLES

Government-supported initiatives to close the digital divide in Tasmania will align with the following principles

- ***Accessibility:*** more equitable coverage and connectivity
- ***Ability:*** inclusive strategies for digital literacy, knowledge and skills
- ***Affordability:*** digitally-delivered essential services within reach of all

MAJOR ACTIONS

1.1	***Deliver the Digital Ready for Daily Life program for digitally disadvantaged groups, including low income households, older Tasmanians and people not in paid employment***
1.2	***Strengthen opportunities for lifelong digital skills learning***
1.3	***Provide more options and opportunities for public access to 'anytime, anywhere' government services***
1.4	***Improve telecommunications infrastructure, particularly in rural and regional Tasmania***
1.5	***Increase 'smart city' technology to support urban communities and new technology businesses***
1.6	***Support transformative digital projects that improve the delivery of frontline services to Tasmanians***

PRIORITY 2

OUR DIGITAL ECONOMY

DIRECTION

Tasmania's economy will be bolstered by the competitive advantage, productivity growth and prosperity enabled by knowledge-driven digital transformation.

Economic success is intrinsically linked to the ability to embrace and actively participate in the digital revolution. Government can positively influence economic performance through leadership, collaborative partnerships, public education and innovative policies, projects and programs.

Entrepreneurs recognise that Tasmania's size and socioeconomic characteristics allow us to conduct research, pilot new technologies and truly engage with citizens. With interest building momentum, conditions are perfect for the digital transformation of the economy and for establishing and promoting Tasmania as a centre for digital excellence.

To realise the value of these conditions, Tasmania must be well-positioned to foster, attract, train and retain a highly skilled pool of local professionals and a technology-driven workforce.

The digital engagement of Australia's small-medium businesses has accelerated significantly.[3] Businesses are increasingly adopting new technologies to respond to the needs of customers and suppliers, and to achieve regulatory compliance. These technologies offer significant prospects for economic growth, helping to overcome geographic challenges and open up previously inaccessible national and global markets for Tasmanian businesses, especially for those in more remote and regional areas of the State.

As businesses transform to keep pace with contemporary expectations, they expect the same level of transformation from government. The Government's approach to future service delivery is intended to meet the digital infrastructure and interaction expectations of business and industry sectors, freeing up time, reducing red tape and lowering costs for businesses and government alike.

PRINCIPLES

The Tasmanian Government will support a digitally connected and prosperous business community through

- ***Capability:*** skilled and empowered digital-ready businesses
- ***Creativity:*** accelerated business startups and innovative career pathways
- ***Connectivity:*** strategic goals achieved through collaborative relationships and connected resources

MAJOR ACTIONS

2.1	***Empower local businesses through the Digital Ready for Business program***
2.2	***Work with industry, business and education partners to develop and promote digital education, career pathways and workforce capability***
2.3	***Accelerate technology startups and entrepreneurial pathways through targeted programs supported by the Office of the Coordinator-General***
2.4	***Build the export capabilities of technology businesses through the Tasmanian Trade Strategy 2019–2025***
2.5	***Uplift the global branding of Tasmania's information technology industry***
2.6	***Work with industry providers to enhance the adequacy and reliability of Tasmania's digital communications infrastructure***

3 Deloitte Access Economics (2017) *Connected Small Business.*

PRIORITY 3

OUR DIGITAL GOVERNMENT

DIRECTION

The Tasmanian community is best served by a progressive government that puts the contemporary needs and expectations of citizens first, transforming the way it works and the way services are delivered.

The Tasmanian Government is developing foundations to support the introduction of digital services that are easy to access, understand and use. We know that people expect to be able to quickly and conveniently access everything they need online, irrespective of age, gender, location, ability, life circumstances or cultural heritage. People in remote and regional communities also understand the potential of digital transformation to minimise geographical barriers to government service accessibility.

The Government's approach encourages the progressive integration of multiple government systems, while ensuring that government-held information and services continue to be securely protected. Significant funds have already been allocated to initiatives supporting joined-up digital services and better personal outcomes for vulnerable children, people and families in need, through projects involving community safety, health, child protection and allied services.

As well as enabling community benefits, digital transformation can realise greater cost efficiencies and productivity benefits for government. The adoption of new technologies and new ways of working can support staff to focus on higher value, more responsive human interaction with clients. There are also greater opportunities for geographically dispersed teams of government workers to deliver seamless and consistent citizen-centric services.

The safe and timely transformation of public-facing services must be founded on new ways of managing, sharing and analysing digital data to enhance evidence-led policy and decision making. To support this, *Our Digital Future* prioritises development of a whole-of-government technology roadmap, cybersecurity maturity, information asset management and digital workforce capability. The Government will also develop a more agile approach to the procurement of technology services, including implementation of a new cloud policy that preferences, rather than mandates, the use of on-island cloud services.

PRINCIPLES

The Tasmanian Government will develop new digital infrastructure and systems that demonstrate

- ***Simplicity:*** intuitive, seamless and convenient services that enhance two-way interaction
- ***Security:*** trusted, resilient systems that safeguard government-held information and services
- ***Strategy:*** connected systems and services that deliver better public outcomes

MAJOR ACTIONS

3.1	***Develop new frameworks for information management and data analytics***
3.2	***Develop a whole-of-government technology roadmap***
3.3	***Adopt a cloud-first policy approach across government agencies***
3.4	***Implement a cybersecurity program that prioritises critical asset protection across government***
3.5	***Develop digital culture and capability across government agencies***
3.6	***Streamline government processes for the procurement of technology services***
3.7	***Reduce government red tape through the adoption of digital solutions***
3.8	***Develop an agile, iterative and risk-managed approach to the management and delivery of digital projects and services***

THE WAY FORWARD

Tasmanian Government agencies are collaborating and actively engaging with Tasmanian people, communities, industries and businesses as we pursue the vision of a prosperous and connected Tasmania, collaborating and thriving in a technology-enabled world.

It is impossible to predict where challenges and technologies will take us in the future, so the frameworks and programs we establish now must be dynamic enough to allow for timely and effective responses to the evolving digital needs and expectations of Tasmanians.

Working on behalf of all agencies, the Tasmanian Government's Department of Premier and Cabinet welcomes input from individuals or organisations on the priorities, objectives and major actions identified in this Strategy.

As work progresses, updates on performance against our objectives will inform the ongoing process of review, refinement and reprioritisation that will characterise the Tasmanian Government as a digitally maturing organisation serving a digitally maturing community.

DEPARTMENT OF
PREMIER AND CABINET

Tasmanian Government

GPO Box 123
Hobart TAS 7001
Phone: **03 6166 3111**
Email: **digital@dpac.tas.gov.au**
Visit: **www.digital.tas.gov.au**

WORK STREAM 1: PROGRESS FOUNDATIONAL WORK

OUR DIGITAL COMMUNITY

		COVID-19 RECOVERY LINK	STATUS
1	Deliver the Digital Ready for Daily Life program for digitally disadvantaged groups, including low income households, older Tasmanians, people not in paid employment	✹✹✹	*Completed*
2	Strengthen opportunities for lifelong digital skills learning	✹✹	*Completed-Ongoing*
3	Provide more options and opportunities for public access to 'anytime, anywhere' government services	✹✹✹	*Completed-Ongoing*
4	Improve telecommunications infrastructure, particularly in rural and regional Tasmania	✹✹	*Completed*
5	Increase 'smart city' technology to support urban communities and new technology businesses	✹✹	*Completed*
6	Support transformative digital projects that improve the delivery of frontline services to Tasmanians	✹✹✹	*In delivery-Ongoing*

OUR DIGITAL ECONOMY

1	Empower local businesses through the Digital Ready for Business program	✹✹✹	*In delivery-Progress*
2	Work with industry, business and education partners to develop and promote digital education, career pathways and workforce capability	✹✹✹	*In delivery-Ongoing*
3	Accelerate technology startups and entrepreneurial pathways through targeted programs supported by the Office of the Coordinator-General	✹✹✹	*Completed -Ongoing*
4	Build the export capabilities of technology businesses through the Tasmanian Trade Strategy 2019–2025	✹✹✹	*In delivery-Progress*
5	Uplift the global branding of Tasmania's information technology industry	✹✹✹	*In delivery-Progress*
6	Work with industry providers to enhance the adequacy and reliability of Tasmania's digital communications infrastructure	✹✹✹	*In delivery-Attention*

OUR DIGITAL GOVERNMENT

1	Develop new frameworks for information management and data analytics	✹✹✹	*In delivery-Progress*
2	Develop a whole-of-government technology roadmap	✹	*In delivery*
3	Adopt a cloud-first policy approach across government agencies	✹✹	*Complete*
4	Implement a cybersecurity program that prioritises critical asset protection across government	✹✹✹	*Complete*
5	Develop digital culture and capability across government agencies	✹✹✹	*In delivery-Not formal*
6	Streamline government processes for the procurement of technology services	✹	*Complete*
7	Reduce government red tape through the adoption of digital solutions	✹✹✹	*In delivery-Progress*
8	Develop an agile, iterative and risk-managed approach to the management and delivery of digital projects and services	✹	*In delivery-Not formal*

WORK STREAM 2: STRENGTHEN COVID-19 RECOVERY & RENEWAL

		COVID-19 RECOVERY LINK	STATUS
1	Review and analyse COVID-19 emergency response learnings and challenges	✹✹✹	*Completed*
2	Collaborate with industry and peak bodies to consider existing proposals and new opportunities	✹✹✹	*Completed*
3	Work with all stakeholders to scope opportunities to support a stronger Tasmania	✹✹✹	*Completed*
4	Monitor, review and refine strategic planning and major action pathways to support recovery and renewal	✹✹✹	*Completed*
5	Support the recommendations and outputs of the Premier's Economic and Social Recovery Advisory Council	✹✹✹	*Completed*

Tasmanian Government

ATTACHMENT 1 - DATA AND DIGITAL SUB-COMMITTEE WORK PLAN 2025

Work Plan Overview

New to the work plan

Completed 2024

	Digital Services	Common Systems and Platforms	Information and Data Management	Cyber Resilience and Risk	Digital Workforce Capability
Flagship Initiatives	MyServiceTAS Portal — ServiceTAS · Support · Done WWVP Update — Justice · Monitor · To do	HR Transformation Program — DPAC · Support · In progress Modernisation of Government Data Networks — DSS · Support · In progress Digital Communications Transformation Program — DSS · Support · In progress MRS Business Case — Monitor · State Growth · Done	PSPF Info-Sec Information Classification — DPAC · State Growth · Support · In progress	Cyber Hubs — DSS · In progress Cyber Security Uplift Program — DSS · Done State Cyber Emergency Plan (SCEP) - — DSS · Done	
Enabling Initiatives	Digital Inclusion Strategy — DSS · Support · In progress Citizen Digital Identity and Credentials - Digital Driver License — DSS · ServiceTAS · State Growth · Support · In progress	Our Digital Future Refresh — DSS · Support · In progress Digital Capability and Technology Roadmap — DDC · Responsible · In progress Employee Identity & Access — Health · Monitor · In progress Critical Systems Infrastructure Investment Plan — DDC · To do	AI Roadmap 2025-2027 — DDC · Responsible · To do Whole-of-government data sharing and access capability — DSS · OSA · Support · In progress Information and data management framework — DSS · OSA · Support · In progress Guidelines for Responsible Use of AI — DDC · Responsible · Done	TAS Gov Cybersecurity Strategy 2024 -2028 — DSS · Support · Done	Digital Workforce Capability Pathway Program — DSS · In progress Digital Careers — DSS · In progress Whole-of-Government Vendor Panel for Professional Services under the Direction of the Customer — DSS · Health · In progress

Flagship initiatives supported by DDC

Ref	Initiative	Stream	Alignment	Lead OU	Status
22/02	**Human Resources Transformation Program (HRTP)** DDC continues to provide advice, support as required. Name change from HRIS. In 2020, the Tasmanian Government approved a HRIS Business Case which sought funding to replace many disparate HR systems, for the Department of Health (DoH) with the potential for it to be a precursor for a single integrated solution across the State Service. Program has moved on to whole of government implementation coordinated by SSMO in DPAC. Whilst the program is focused on transformation change in HR, the program is dependent on establishing the supporting software to deliver services along with data and digital infrastructure.	Common Systems and Platforms	TSSR 22, 34 Keeping Children Safe	SSMO (DPAC)	Health continuing with its implementation. The critical CMS module has been rolled out across government. New governance arrangements in place to support whole-of-government outcomes. Work underway to procure system integration and application management services. Program implications for – reporting, analytics and insights, data governance and integration. Multi-year program
22/04	**Modernisation of Government Data Networks** Evolve services to meet agencies requirements and the adoption of new and emerging technologies, including establishing a new panel arrangement for modern data and internet services.	Common Systems and Platforms	TSSR 22 ODF 1.4, 3.3	DSS (DPAC)	Governance in place with DDC oversight, program is progressing – core upgrades, new network security framework, new data and internet panel, enhanced DDOS controls. Multi-year program
22/05	**Digital Communication Services (DCS) Service Model Transformation (SMT) Project.** DDC provides oversight and governance. Formally Telephony Transformation Program. Replace the existing telephony service arrangements within government with a new operating model with access to contemporary communications platforms and solutions.	Common Systems and Platforms	TSSR 22 ODF 3.3	DSS (DPAC)	Phase 3 definition completed – detailed service model design is complete and endorsed by key stakeholders. Progressing through tender evaluations and contracts becoming available for transition mid to late 2025. Multi-year program.
22/15	**Protective Security Policy Framework – InfoSec** DDC provides advice and support on INFOSEC module. The development and implementation of a Tasmanian PSPF will establish whole-of-government policy requirements and guidance on implementing and maintaining effective protective security practices	Data and Information Management	ODF 3.1 Keeping Children Safe	RRT (DPAC)	DDC members collaborated with OSEM to help develop the INFOSEC module. Email Information Classification validation work completed by DPFEM in 2022 Information Classification implementation pilot underway at DPAC.
22/20	**Cyber Hubs** Develop and validate a whole-of-government functional leadership solution for cyber security by establishing a desirable, feasible and viable operating model for managing cyber security risk across government.	Cyber Resilience and Risk	TSSR 21, 23 ODF 3.4	DSS (DPAC)	Project initiation commenced late in 2023, initially disrupted by operational cyber security requirements has now moved through discovery. Next phase is conduct of a pilot to validate a shared incident management process and to implement suggested improvements in whole of government cyber governance and assurance.

Ref	Initiative	Stream	Alignment	Lead OU	Status
25/01	**Registration to Work with Vulnerable People (RWVP) Expansion Program** Aims to enhance protections for vulnerable individuals in Tasmania, the program includes legislative changes and the implementation of a new IT system for better administration and user experience. This will also include improvements in the RWVP system integration with the myServiceTas platform.	Digital Services	Keeping Children Safe	Justice	* New to work plan Tender opened 08/03/2025 for a "Registration and Licensing Solution to support Registration for Working with Vulnerable People".

Enabling initiatives progressed through DDC

Ref	Initiative	Target Outcomes	Stream	Alignment	Lead OU	Status
22/01a	**Our Digital Future Refresh** DDC is a key government stakeholder for this work. Minister for Innovation, Science and the Digital Economy has requested a refresh of the Our Digital Future strategy. This includes a new strategic action plan for digital government. The Strategic Action Plan associated with Our Digital Future has not been updated since 2021. The actions prioritised for Government (Our Digital Government) set priorities for digital in government and are in need of better alignment with current broader government priories. Thes priorities are also needed to guide related work in 22/01b and 22/01c.	To improve the alignment and relevance of strategic actions under Our Digital Future, with more recent priorities of government.	All	Government Priorities Keeping Children Safe TSSR 22, 24, ~~19~~	DSS (DPAC)	* New to work plan DDC had undertaken work to review a possible update to the original action plan. Work will now progress through a consultation process with community, industry and government stakeholders. The Secretaries Board will be engaged to articulate their digital ambitions for Government.
22/01b	**Digital Capability and Technology Roadmap** Develop an abstract visualisation that depicts how capabilities are aligned and integrated to deliver on the government's priorities. Key domains of capability would ideally be set out with strategic directions/vision, lifecycle and implementation status, current roadmaps, and active initiatives**.** This is a core strategy and planning artifact to support the establishment of a Platform Based Functional Leadership Model based on capabilities and provide agreed roadmaps for those capabilities.	Contribute to establishing platform-based functional leadership. Improve leadership and direction for agencies planning digital investments. Provide transparency with respect to government strategies and future proposals. Assist to deliver integrated customer journeys, as opposed to siloed digital services.	All	TSSR 22, 24, ~~19~~ Keeping Children Safe ODF 3.2 ICT Strategy, Critical Systems, and Investment Audit 2020 Digital Initiatives Audit 2023.	DSS (DPAC)	Work has not significantly progressed on this initiative due to time and resource constraints and the need to articulate the roadmaps as part of plan or digital priories for government. Notwithstanding there is agreement amongst DDC members that setting light weight strategic directions for critical digital capability priorities offers a pathway forward. Demonstrator strategic directions documents for digital identity and credentials, digital communications, data networking, and cyber security have commenced drafting.

Ref	Initiative	Target Outcomes	Stream	Alignment	Lead OU	Status
22/11	**Digital Inclusion Strategy** Establish a working group to oversee the coordination of digital inclusion initiatives across government and to develop an initial strategy, a roadmap and KPIs to progress improvements in digital inclusion. Acknowledging that there are programs already underway across government (from a delivery perspective) that need to be incorporated into this work.	• Increased understanding of the current digital inclusion initiatives being implemented across government. • Improved communication of information relating to digital inclusion initiatives to external stakeholders. • An agreed and coordinated set of for digital inclusion priorities for Tasmania. • An ability to measure and validate the performance and value of digital inclusion initiatives. • Increased understanding of how the core dimensions of digital inclusions impact disaster resilience.	Digital Services	TSSR 65 ODF 1.1 PESRAC	DSS (DPAC)	Originally funded in 2023 budget. Considerable work across Internal stakeholders. National alignment and information sharing via DDMM working groups, and inter-jurisdictional CIO forum. Internal Community of Practice established. Internal strategy drafted and maintained from Q2 2024, although strategy endorsement delayed due to election changes of ministers and a review initiated in DECYP. External forums with industry and community sector to be held H1 2025 and integrated with the Our Digital Future refresh.
22/16	**Revised framework for whole of government information and data management.** In consultation with key stakeholders, develop a new / revised framework that addresses critical aspects of information and data management – leadership, strategy, governance and information asset management. Additionally, as part of the strategy development facilitate the development of an agreed plan and roadmap to establish the foundational capability for information management, sharing and linkage across government. This initiative is a dependency for 22/14.	• Improve whole-of-government coordination of data and information management. • Provide reusable capabilities to address existing and emerging government priorities for information sharing and data linkage.	Data and Information Management	~~TSSR 19~~ TSSR 5,9 ODF 3.1 Keeping Children Safe (COI 19.8(1))	OSA (DECYP) DSS (DPAC)	A Working group was originally established in Q4 2022. Considerable work has been undertaken with limited resources in DSS and in-kind support from the State Archivist and other agencies. A draft strategy and roadmap were developed with a view to addressing key governance, leadership and asset management issues at a whole of government level. Options were also developed to establish an operating model. Feedback from Secretaries Board in Dec 2023 asked that we seek greater alignment with work linked to Keeping Children Safe Strategy. An updated approach linked to the Keeping Children Safe Strategy will be finalised in Q2 2025.

Ref	Initiative	Target Outcomes	Stream	Alignment	Lead OU	Status
22/22	**Digital workforce capability pathway program** Develop a whole of government digital workforce capability development framework and roadmap that is aligned to government priorities and risk, supporting the vision for digitalisation reform outlined in Our Digital Future and the Tasmanian State Service Review. The roadmap outlines targeted strategies and initiatives that align with three key focus areas: Digital skills profiling and workforce planning; Digital careers development; and Digital talent pipelines aimed at addressing the TSS digital (including data and cyber) workforce challenges and maximise on opportunities.	• Improvement in the Tasmanian Government's ability to attract, recruit, develop and retain its digital workforce. • Alignment of digital and ICT skill descriptors in job roles with national and international standards – Skills Framework for the Information Age. • Improve the understanding of our workforce skills profile and empower individuals to understand and plan their own path for growth within the digital and ICT professions.	Digital Workforce Capability	TSSR ~~40~~, 41 ODF 3.5	DSS (DPAC) SSMO (DPAC)	DSS initially developed a long-term plan and roadmap to address some of the core issues with the digital workforce. Work was also initiated work to establish an intern program, improve the graduate recruitment process, aligning ICT and cyber-SODs with an international standard known as the Skills Framework for the Information Age (SFIA). Additional work was also undertaken to improve gender, cultural and age diversity within TSS. DSS has also worked with SSMO and other states, territories and the Commonwealth to share and assimilate good practices. TAS Gov is seen as a leader in applying SFIA to employee skills profiles and has garnered significant support from the Australian Computer Society and the Australian Public Service Digital Profession in this area. Working with industry to benefit broader Tasmanian Digital, ICT and cyber workforce ecosystem. Ideally, we are looking to move this work into a core action within the refreshed Our Digital Future and expand the practices beyond government into industry and for learners.
24/23	**Digital Careers** A schedule of work for 2025 to support the promotion of digital careers within the TSS, through industry and community events and related initiatives.	• Increased awareness of digital career pathways across the community. • Increased support for School/College/ICT Career Pathways programs being run by DECYP.	Digital Workforce Capability	Manage strategic risk and opportunities.	DPAC	* New to work plan This initiative requires a review pending recent government announcements regarding "right sizing" the workforce.

Ref	Initiative	Target Outcomes	Stream	Alignment	Lead OU	Status
22/08	**Citizen Digital Identity and Credentials: Digital Driver License** This initiative has pivoted towards establishing a pathway for the introduction of digital driver licenses in Tasmania. Initial work had focused on governance and stakeholder engagement for the use of digital identity and credentials with Government services, and to build a policy foundation to support and embrace digital identity and credentials at a national level. The pivot to focus on digital driver licenses was undertaken to align the objectives of establish capabilities to support digital identity and credentials with directly attributable community outcomes and benefits.	Leverage the benefits of digital drivers licenses for the community: • Create a better experience for driver license holders, making it easier, more convenient and more secure for Tasmanians to manage their driver license and identity credentials. • Improve the efficiency of managing and verifying driver licenses and identities, by streamlining processes and reducing delivery costs. • Address future opportunities and risk – better position Tasmania to engage and participate in the digital economy initiatives linked to the use of digital identity and credentials.	Digital Services Common Systems and Platforms	TSSR 25, 65 ODF 1.7	DPAC DSG	DSS has considerable involvement with the Commonwealth forums and an independent inter-jurisdictional forum on digital ID and verifiable credentials. DSS and DSG have engaged with Austroads for the design and testing of an interoperable digital driver license. Strategic Infrastructure Investment Proposal (SIIRP) has been prepared seeking funding to further understand the options and develop a detailed business case for future government investment.
24/12	**AI Roadmap 2024-2026** With the completion a preliminary roadmap for AI the end of 2024, the Data and Digital Committee convened an AI roundtable to agree on a new set of recommendations for taking the AI agenda forward at the whole-of-government level. Recommendations and priorities were developed to inform a new 2-year roadmap for AI through to 2027.	• Establish directions and deliver whole-of-government AI policy • Understand the opportunities for Government • Increase collaboration and knowledge sharing for AI • Adapt procurement and technology sourcing controls to address risk and opportunity in AI • Establish longer term governance for AI	Data and Information Management	Manage strategic risk and opportunities	DPAC	* New to work plan New working group established, Workplan focused on target outcomes to be progressed. With Government focus on efficiencies it is expected that the roadmap might require uplift to explore use cases for AI that can facilitate automation and productivity improvement.
24/13	**Whole-of-Government Vendor Panel for Professional Services under the Direction of the Customer** Establish a whole of government panel for ICT professional services labour hire i.e. a contract for services under the direction, control, and supervision of the customer.	• Streamline the procurement process for critical resources • Enhance the responsiveness of Government Departments to meet urgent project demands.	Digital Workforce Capability	Manage strategic risk and opportunities	Health DPAC Treasury	* New to work plan Requested sent to Treasury to provide implementation guidance and support.
25/02	**Critical Systems and Infrastructure Investment Plan** Establish a whole of government critical systems register, extend the register into an investment plan.	• Improved understanding of risk associated with critical government ICT systems and infrastructure.	Common Systems and Platforms	Manage strategic risk and opportunities	DSS (DPAC)	* New to work plan Register is initial focus, moving on to an investment plan once the register is populated. Exploring the use of SAP LeanIX as an information repository.

Ref	Initiative	Target Outcomes	Stream	Alignment	Lead OU	Status
22/03	**Employee Identity Access Management (IdAM)** Health are currently progressing work for contemporary IdAM solution that could potentially be used by whole-of-government.	• Single employee identity management for whole-of-government, including integration of identity with the Human Resources Management System.	Common Systems and Platforms	TSSR 22, 34 HRTP	Health	DOH are positioning to provide Whole of Government options in contracts.

Potential Future Initiatives

Ref	Initiative	Stream	Alignment	Lead OU	Status
22/10	**Establish a whole-of-government Digital/ICT Services Catalogue** Publish and maintain a catalogue of whole-of-government services (government-to-government)	Potential Future Initiatives	TSSR 24, 65 ODF 3.5	DSS (DPAC)	Concept only, easy to implement, significant support
22/09	**Digital service design and delivery standards** Develop standards to guide digital service design and solution delivery. Based on human centred design principles.	Potential Future Initiatives	TSSR 65 ODF 3.5, 3.8	Government Services (DPAC)	Concept only
22/14	**Whole-of-government information sharing and access capability** Establish a whole-of-government capability for sharing, accessing, linking and analysing data. Establish a formal governance model, system ownership and assign a functional leader to deliver services to, and/or build capability across, all agencies. This initiative is dependent on 22/16	Data and Information Management	~~TSSR 19~~ TSSR 5, 9 COI indirect priority ODF 3.1	Linkage/National Accreditation – DSS (DPaC) Other - TBA	HRTP may establish some of the foundational capabilities Data Linkage capability and associated National accreditation is currently being investigated to support national data initiatives such as NDDA, FDSV and Human Services Youth at risk. Seeking to have capability/accreditation within 12 months
22/06	**Whole-of-government Digital Workplace** Establish a common digital operating environment for the majority of TSS employees – common hardware, software and communications tools.	Common Systems and Platforms	TSSR 5,9		Concept only
22/17	**Functional leadership for spatial and location intelligence capabilities** More detailed exploration of the options for shared spatial and location intelligence capabilities and platforms.	Common Systems and Platforms	TSSR 22		Concept only
24/01	**Whole-of-government policy and standards library** Provide central repository of data and digital standards and policies.	Common Systems and Platforms		DPAC	Concept only, easy to implement.
24/02	**Whole-of-government Learning Management System** Standard learning management platform for whole of government.	Common Systems and Platforms			Concept only
24/03	**Contract Negotiation** Establish a contract negotiation capability.	Common Systems and Platforms		Health	Concept only, access to skills and capability for large scale procurements and contracts are becoming critical.

Ref	Initiative	Stream	Alignment	Lead OU	Status
24/04	**Microsoft Strategic Platform Management** Establish a program to coordinate the sourcing adoption of Microsoft products and services to meet the objectives of PSPF and COI. Design services to meet agencies requirements for interoperation and security in the Microsoft ecosystem.	Common Systems and Platforms		DPAC, Treasury	Concept only
24/05	**IT Service Management** Explore options for consolidating the number of IT Service Management Platforms (ITSM) across government. DOJ recently procured Service Management System that could be broadly procured by other TSS Agencies, without the need to repeat an RFT exercise. DECYP and DEPFM also utilise the Service Now platform.	Common Systems and Platforms		Justice	Concept, with interest from several agencies.
22/01c	**Digital/ICT Investment and Assurance Framework.** Investigate suitable options to establish a framework for investment and assurance associated with strategic or high risk digital and ICT investments. The framework would be used to provide guidance and advice on investment value (desirability, feasibility, viability) and monitor the performance, risk and benefit realisation of initiatives. NB: This initiative would include the implementation of a digital initiative tracker per the Digital Initiatives Audit 2023 report. Enable effective decision making for digital investments at a whole of government level. Ensure the establishment of connected and interoperable systems, platforms and services. Facilitate the efficient use of common systems and platforms.	All	ODF 3.2 ICT Strategy, Critical Systems, and Investment Audit 2020 Digital Initiatives Audit 2023.	DSS (DPAC)	DSS has undertaken discovery work across Commonwealth and States and Territory governments on assurance frameworks, including detailed briefings from NSW Government and Commonwealth (DTA), We are preparing a request for research and advice from out advisory partner Gartner.

Completed Initiatives 2024

Ref	Initiative	Stream	Alignment	Lead OU	Status
22/07	**Service Tasmania Customer Experience Program (myServiceTas)** Development of a digital Service Tasmania portal to provide Tasmanians with a secure and easy-to-use access point for Government services. There are two stages for this program – redevelopment of the Service Tasmania website to make it easier for Tasmanians to find the government services they need; and the development of an initial digital service portal which builds on the new website by providing a personalised customer account and access to initial digital citizen services.	Digital Services	TSSR ~~65,~~ 5, 22 ODF 1.3,1.7	Service TAS (DPAC)	Completed MyServiceTas Portal Goes live Q2/2024 Service TAS website experience updated in 2022. Service TAS has a strategy and roadmap to add more capabilities/services.
23/03	**Guidelines for the Ethical and Responsible Use of AI** To provide interim guidance for agencies to ensure a consistent baseline approach to the use of artificial intelligence in Tasmanian Government.	Data and Information Management	ODF 3.1, 3.8	DSS (DPAC)	Completed Working group established, work is aligned with the DDMM National AI working group national guidelines.
22/23	**Review Communities of Digital Practice** Establish desirability, feasibility, and viability of various Digital CoPs, assist to renew and promote those with good value propositions.	Digital Services	TSSR 47 ODF 3.5, 3.8	DSS (DPAC) noting SSMO looking at all CoPs	Completed There are a number of old groups no longer active or relevant (short lived topics). Considerable success with the Design Thinking and Change Management groups. Recently established a Digital Inclusion Community of Practice and Citizen ID reference group (ran as a CoP). Digital Inclusion Community of Practice, Data and Information Management Working Group and Citizen Identity Reference Group calendars and updated terms of reference have been circulated. Full Calendar will be tabled with the DDC for information.
23/01	**Tasmanian Government Cyber Security Strategy 2024-2028** Review the existing Tasmanian Government Cyber Security Strategy via a cross-functional (business and technical) and cross-agency working group	Cyber Resilience and Risk	TSSR 21, 23 ODF 3.4	DSS (DPAC)	Completed, released Feb 2025 Undertook extensive internal and external stakeholder consultation.
23/02	**State Cyber Emergency Plan (SCEP)** Development of an emergency management plan under the TEMA framework to manage cyber emergencies – incidents that require cross government collaboration and resourcing to manage incident and consequences.	Cyber Resilience and Risk	TEMA	DSS (DPAC)	Completed Plan complete, exercised and used operationally. Waiting to formalise final acceptance with SEMC.
22/18	**Whole of Government Cyber Security Uplift Program** A four-year program established and funded in FY2020/21 to address a number of critical cyber security risks. Includes projects to deliver – vulnerability management for public facing services, incident response capability, education, training and awareness, and agency guidance for cyber reliance.	Cyber Resilience and Risk	TSSR 23 ODF 3.4	DSS (DPAC)	Completed Key deliverables met after a slower than expected start. Still work to complete H2 2024, work focused on vulnerability management, information sharing/observability, training and awareness.

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.

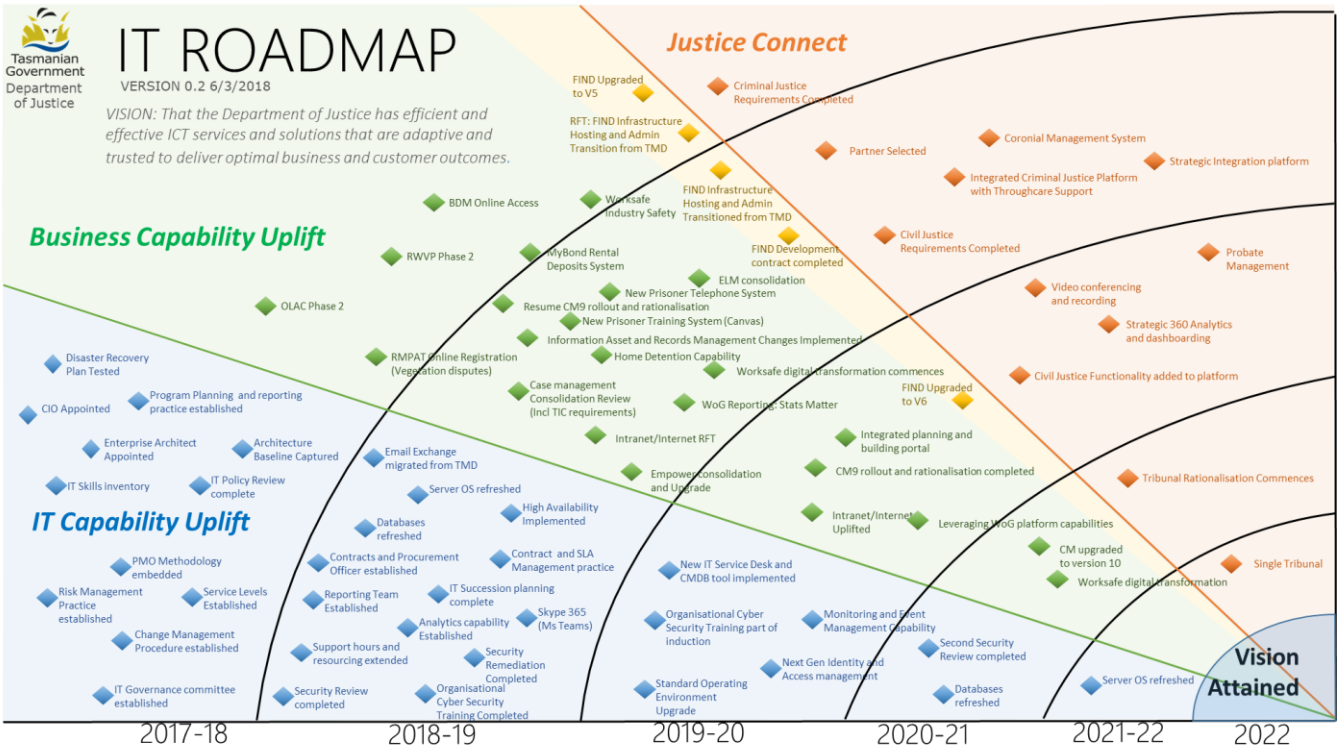
	Current State	Target State	Getting There	Benefits to Agency and Outputs
Systems	• No enterprise architecture • Siloed and aged solutions • Minimal integration • High manual effort • Lack of support 21% of systems are not formally supported • 40% of systems over 10 years old, some as old as 28 years	• 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.

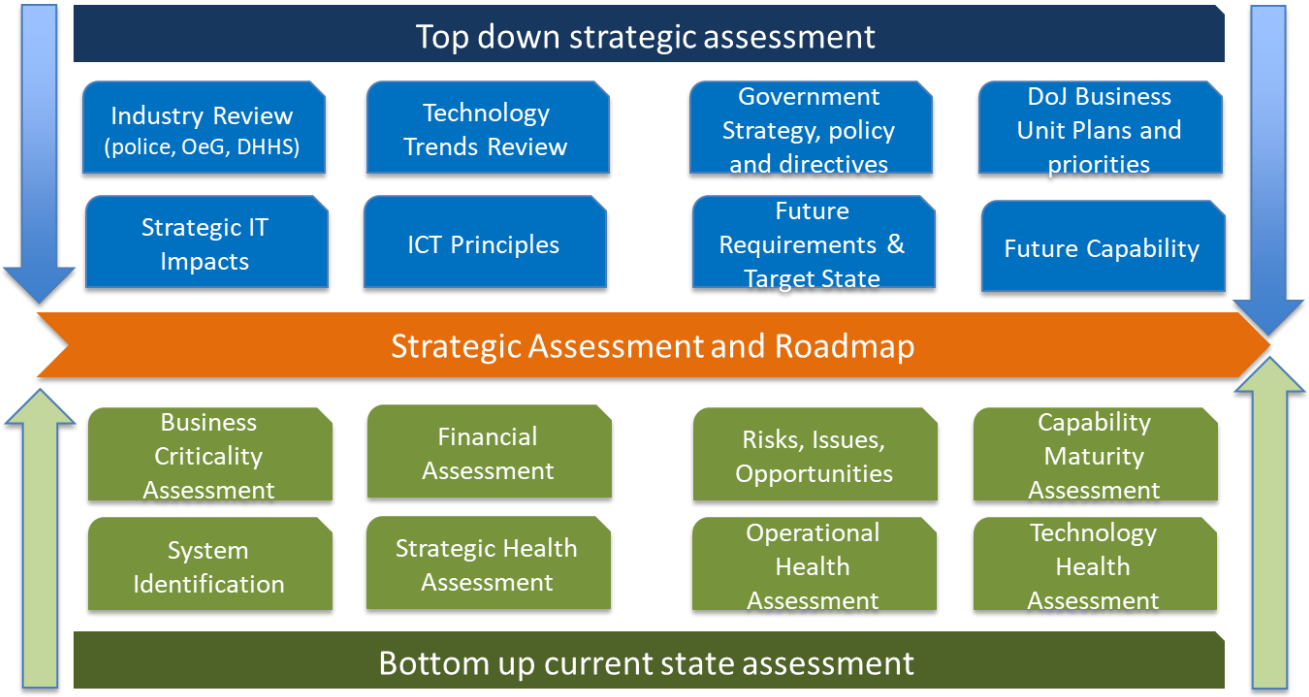
As such, the ICT Strategy has been developed from two viewpoints:

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:

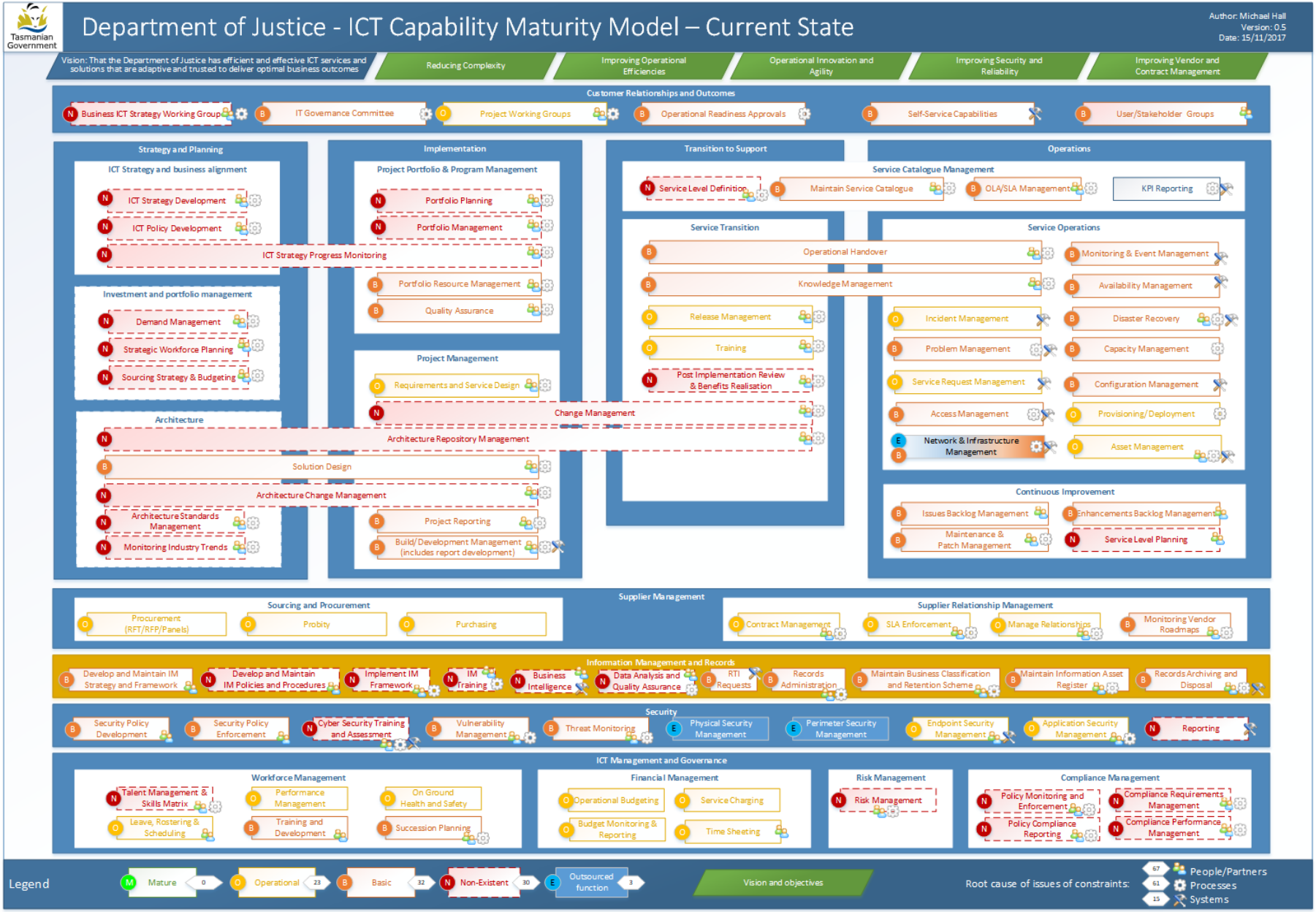


The assessment process was conducted over ten weeks in late 2017, and included interviews with output managers, key system users, the ICT and Projects and Information Teams, and external parties such as Tasmania Police, and the Office of e-Government. In addition to interviews, technical and financial 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;

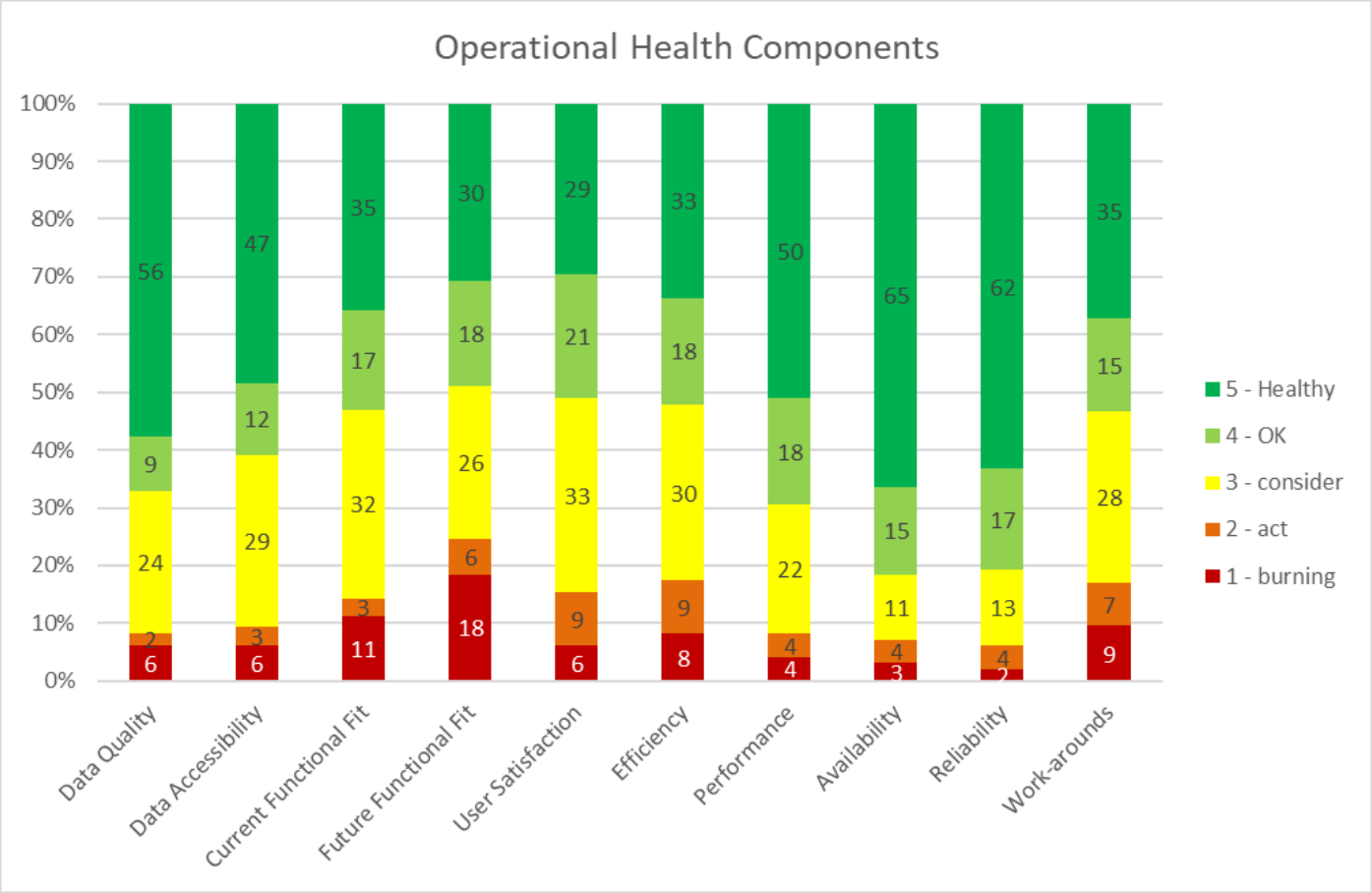
- 21% of systems lacking ongoing vendor support including 17% of business critical systems (increasing operational risk);
- 40% of business critical systems are over 10 years old, and there are some systems that are as old as 28 years; and
- inability to adapt the system to changing requirements.

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.

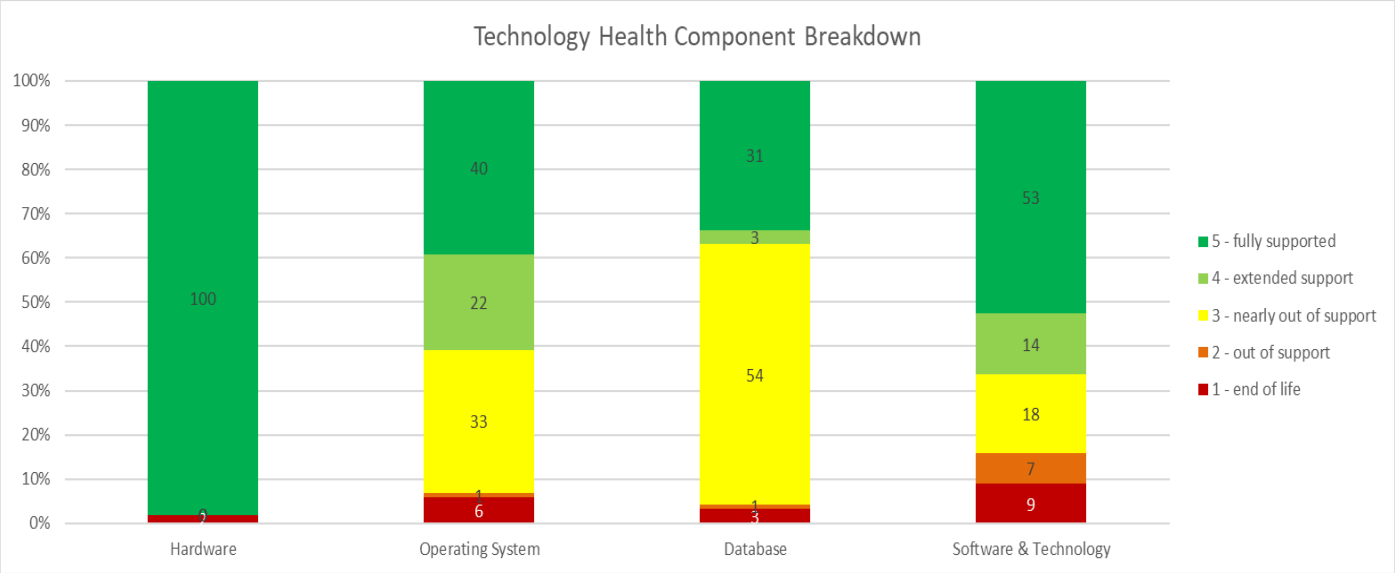
The final outworking of this scenario is that the quality of data is not sufficient to support critical processes, and there have been a number of issues that have drawn negative media and Government attention.[3] Independent reviews into these issues have consistently pointed to underlying gaps in system 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;

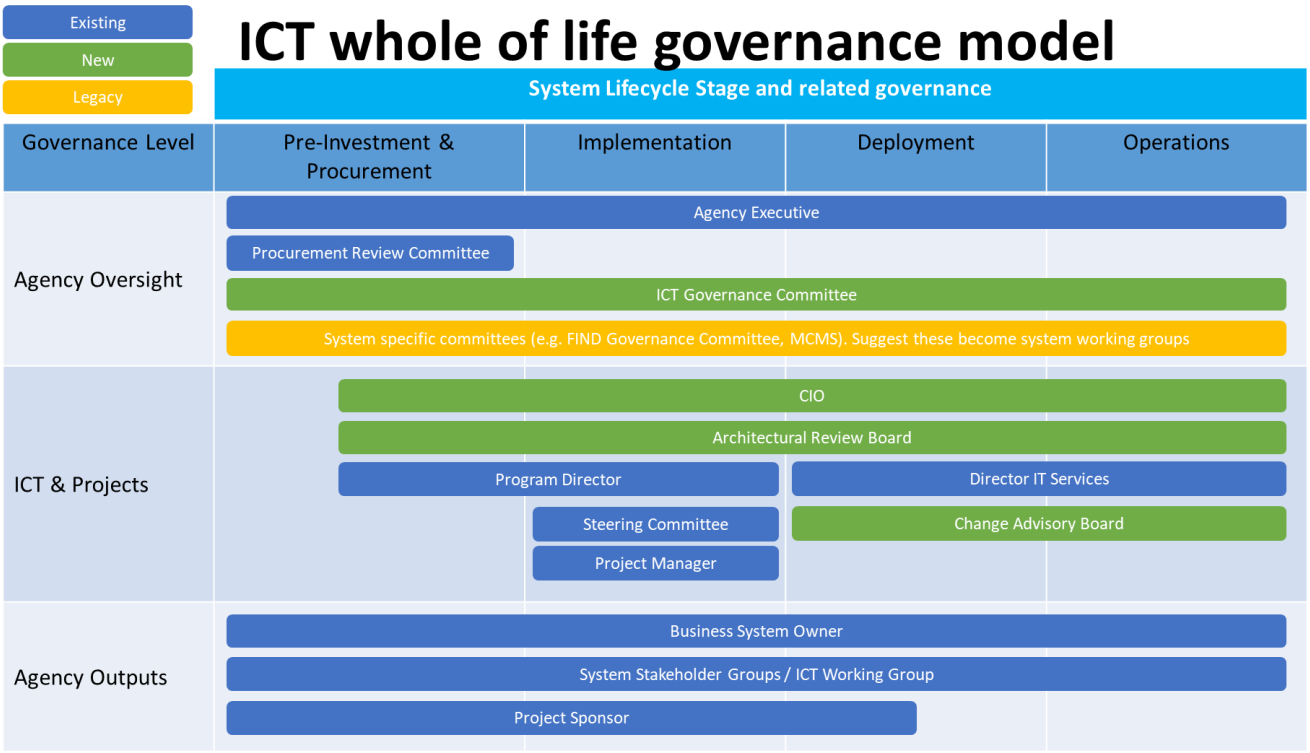
- Overall ICT budgetary ownership and transparency;
- Proactive management of vendors, their capabilities, performance, costs and strategic importance;
- Service Levels being defined, monitored and managed; and
- Understanding the cost of IT through development of a future IT funding model.

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

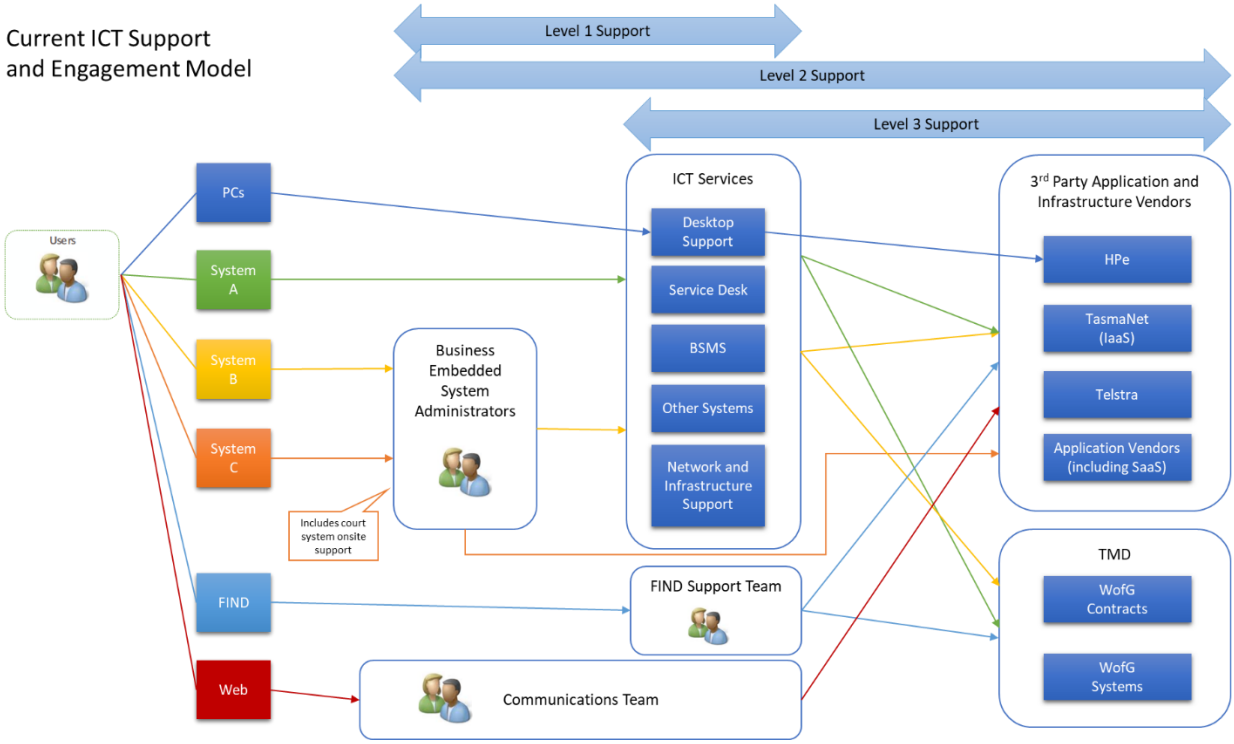
9.1 Current state

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.



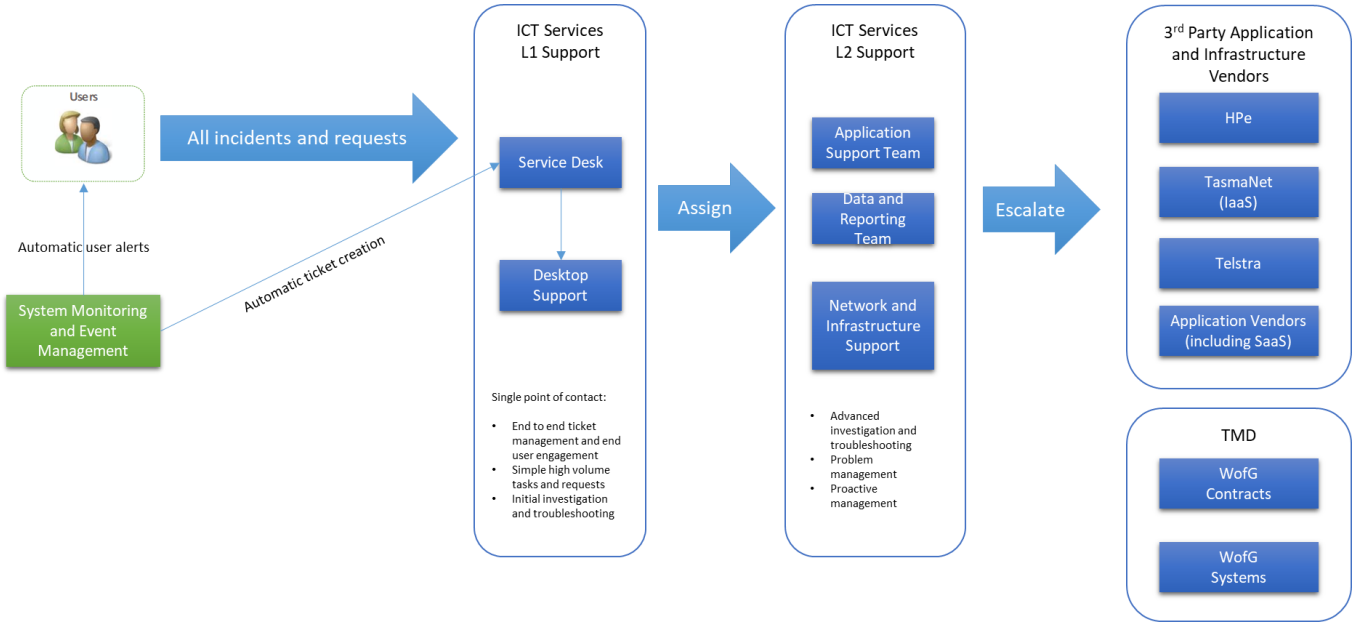
9.2 Target State

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

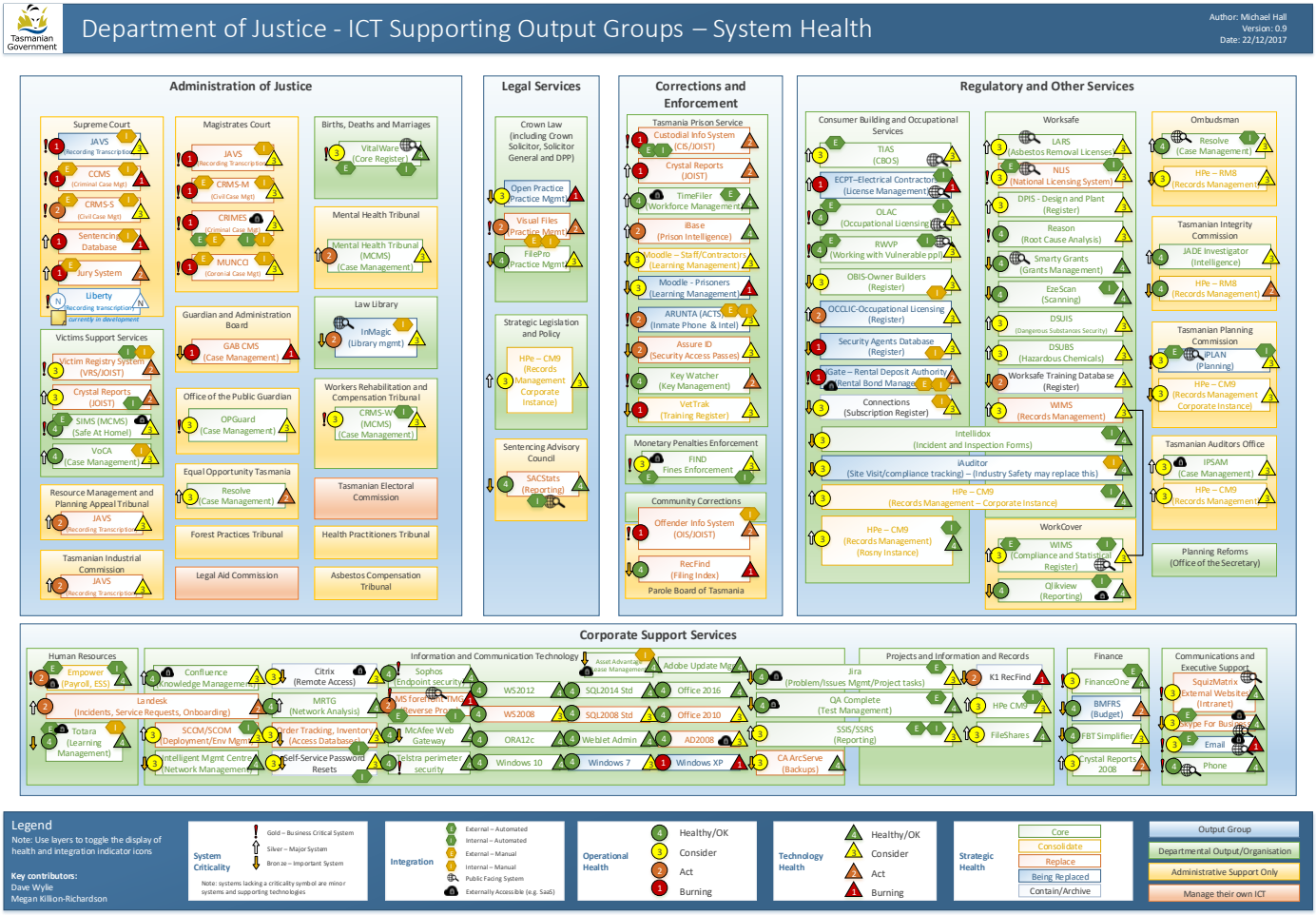
11.1 Current State

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:



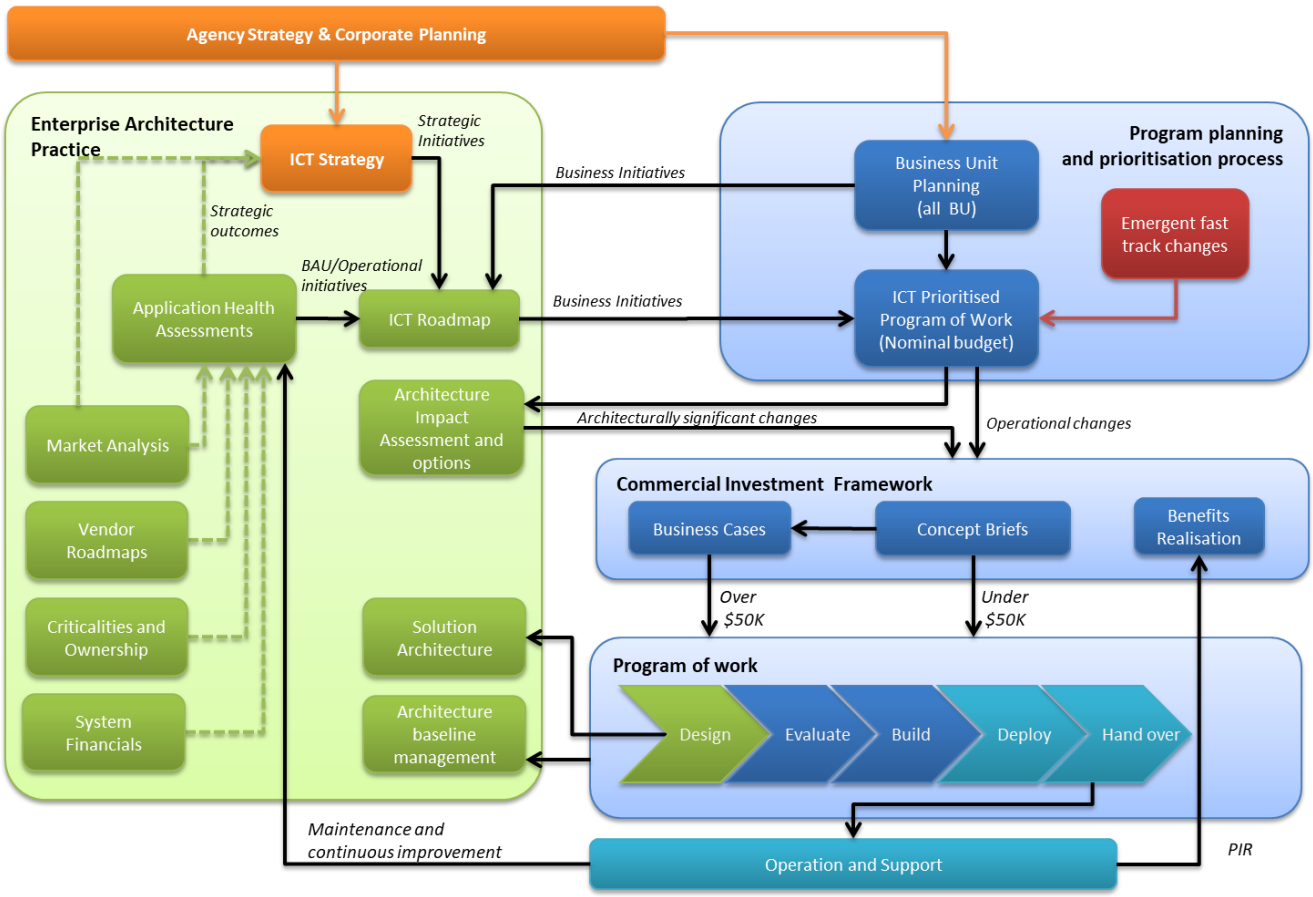
A number of systems can be seen as requiring urgent attention to either upgrade, replace or consolidate, and some systems carry significant risk. In their current state, many of the systems are unable to enable the realisation of the ICT vision or objectives. A remediation plan has been developed with 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.

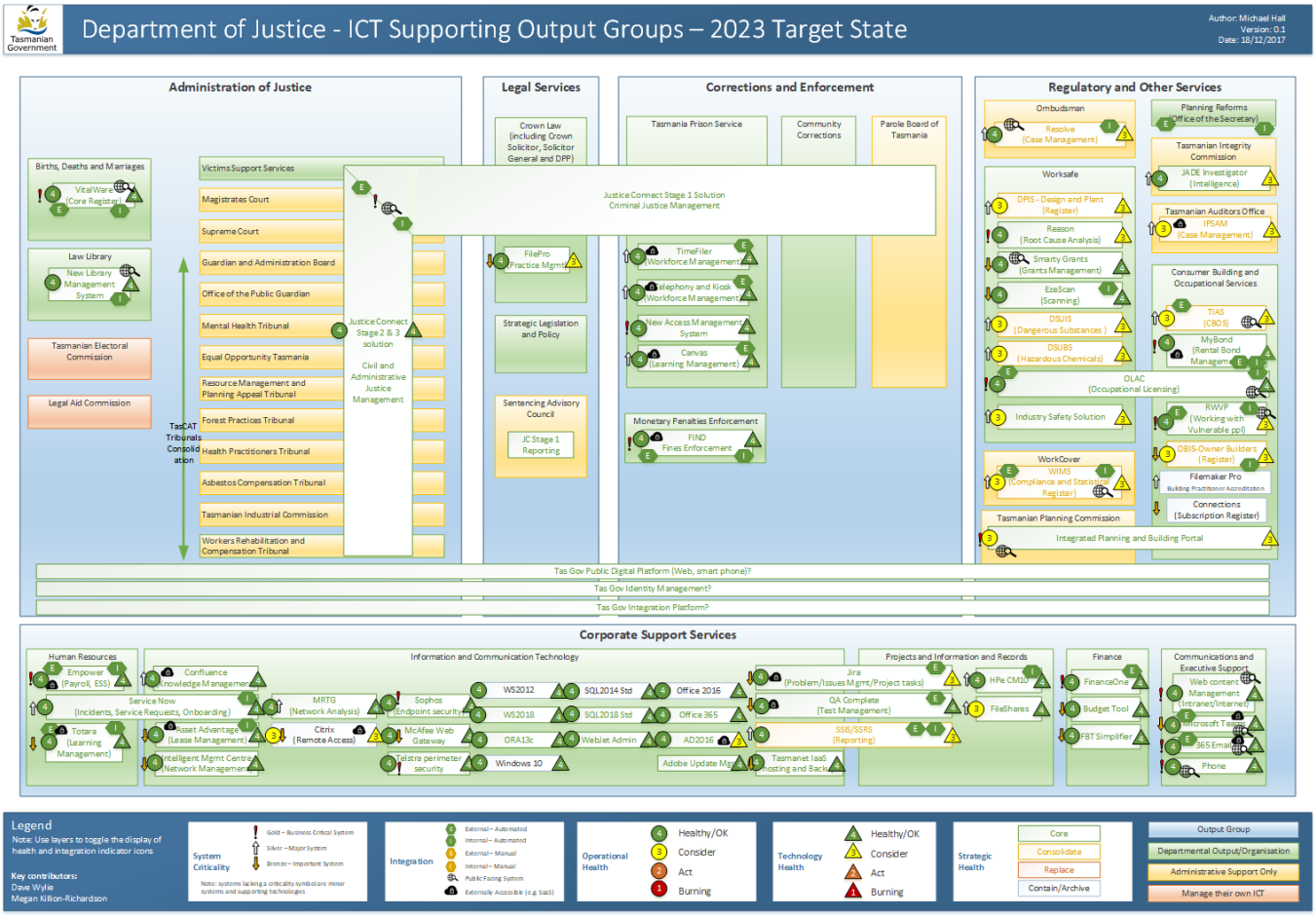
An ongoing integrated approach involving strategic planning, program management, and continuous improvement through support and feedback is required, as illustrated in the diagram below:



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:

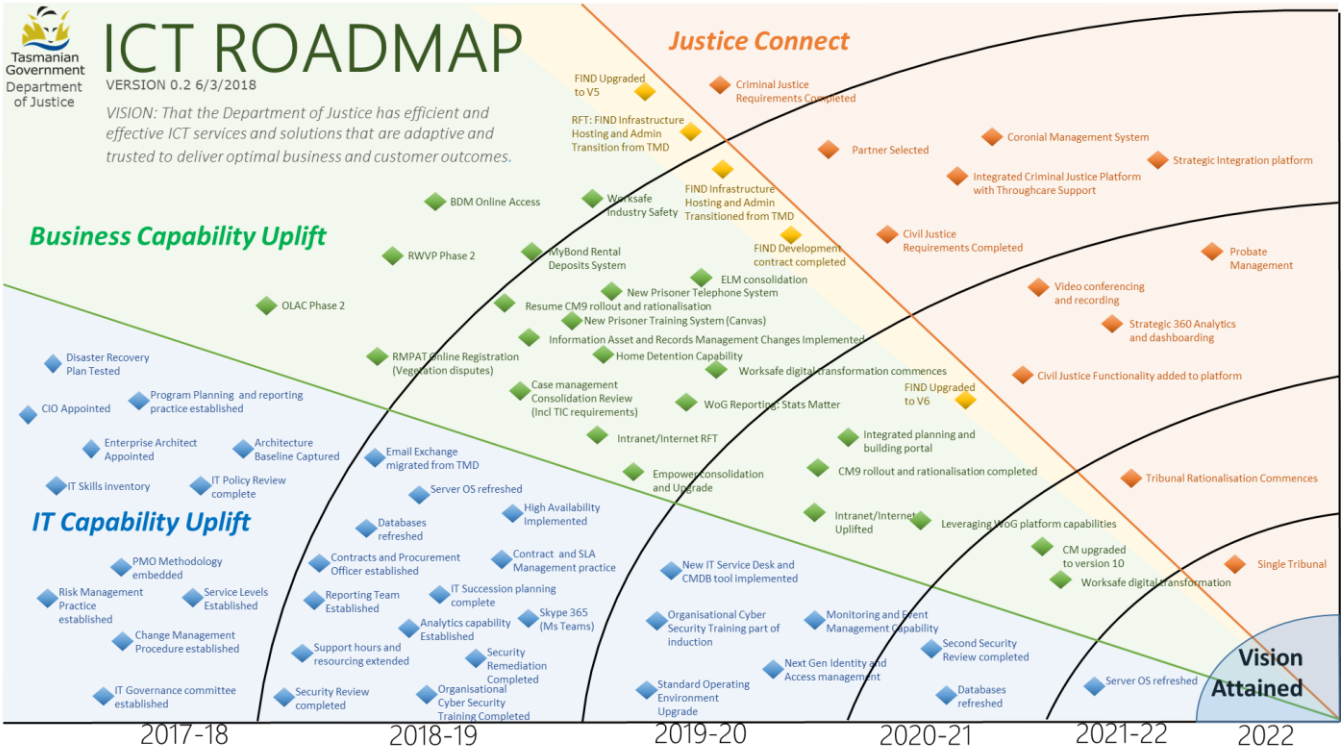
- Introducing capacity management;
- Reviewing the existing deployment and capacity and optimising;
- Independent review of SQL Server database architecture and optimisation for performance and best practices;
- Creation of a disaster recovery plan, and underlying mechanisms, which may include:
    -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

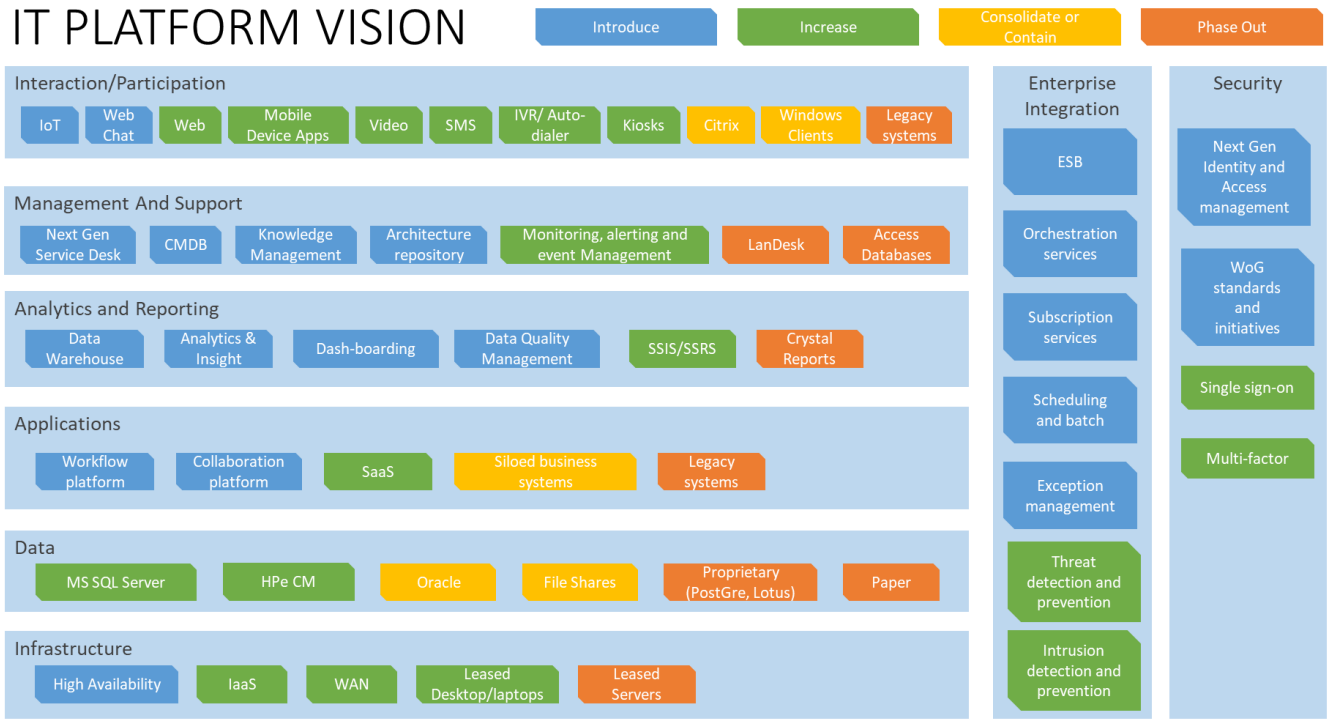
Continuing to lease desktops and peripherals will allow the agility that will be required to keep up with the fast-paced changes in technology, whilst avoiding stranded assets.

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

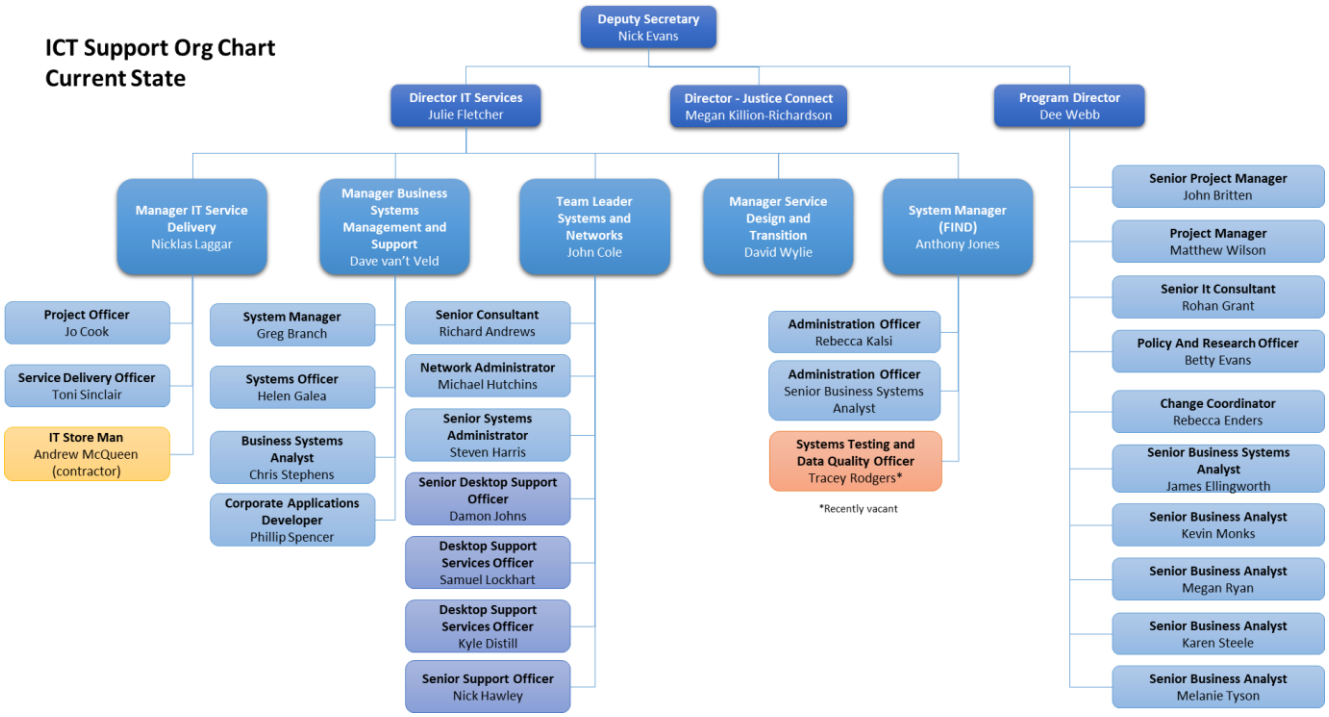
The following assumptions have underpinned this strategy:

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.

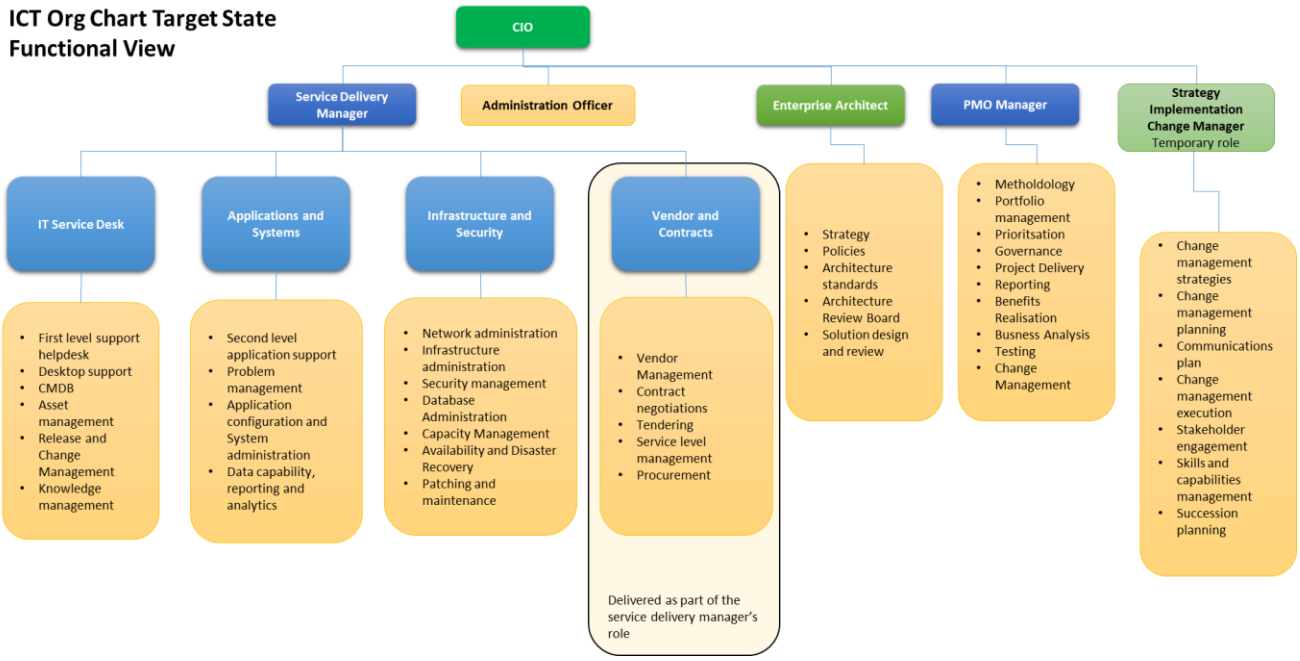
The structure itself is depicted below:



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.

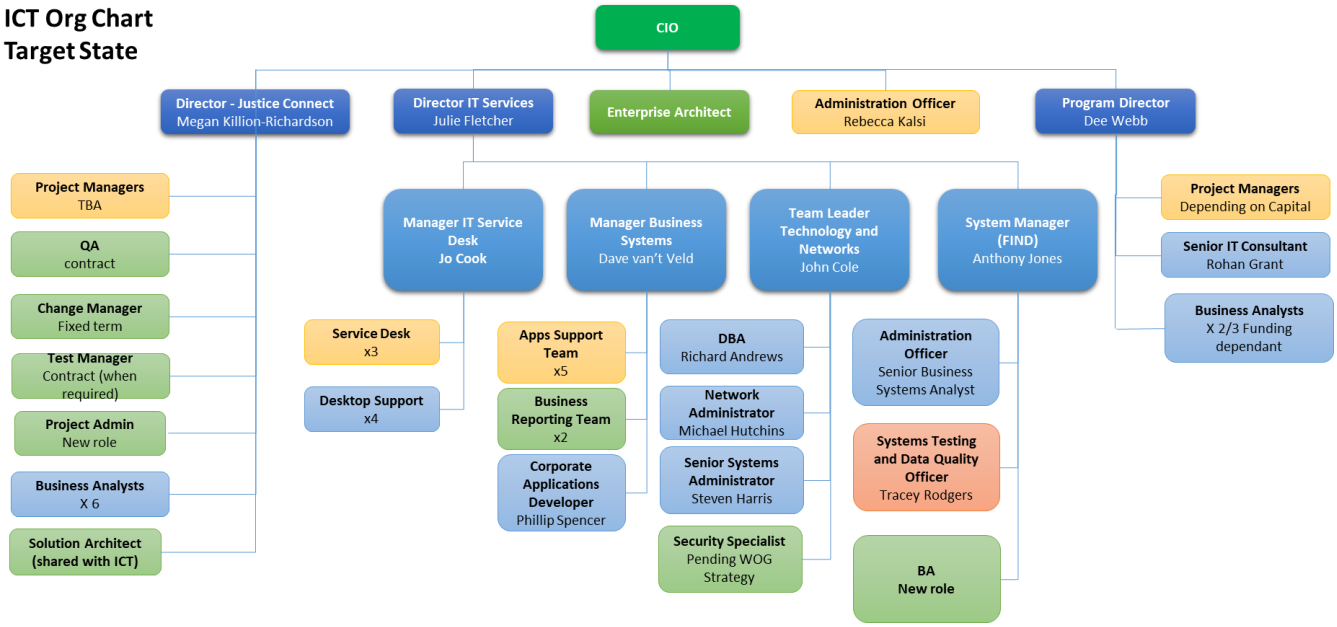
Below is the proposed functional target state:



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

Digital & Data Services Strategic Roadmap 2024 - 2027

Attachment F

The NRE Tas' Strategic Plan has six Strategic Priorities. Strategic Priority activity 6.6.2 is to develop and implement an IT roadmap. This document details that roadmap.

Digital and Data Services will contribute to the delivery of NRE Tas strategic priorities primarily through Strategic Priority 6 and Strategic Priority 1.

Our Purpose

Delivering a sustainable Tasmania

Vision:

A Tasmania where our natural resources, cultural values and environment are recognised and used sustainably to support our future prosperity.

NRE Strategic Priority 6

Building a high performance department, driven by our people and our systems.

NRE Strategic Priority 1

Enable business and employment through sustainable growth of Tasmania's industries.

Whole of Government

To implement the Tasmanian Government's digital and data priorities.

6.6 Driving smart investment in systems and tools that align with our strategic priorities.	6.6.3 Developing and implement a protective security plan for our people, information and assets.	6.4 Embracing innovation and driving continuous improvement in our work practices.	6.5 Establishing a service delivery model that ensures customer and stakeholder centric outcomes.	1.3 Capturing and sharing data and information to support and inform industry and government decision making.
BUSINESS FIRST	**SECURE & RELIABLE**	**FUTURE FOCUSED**	**SEAMLESS EXPERIENCE**	**INFORMATION CULTURE**
To understand our business processes and provide services to meet their diverse needs.	Protect the integrity of the Department's information and technology assets.	Lead the delivery of innovative services and solutions for the Department.	Equip our workforce to be productive, mobile, interoperable and secure.	Maximise the ability to make better decisions through information and insights to our business.

Collaborate with government departments and partners to implement Tasmania's digital and data priorities.

- Information and Data Management Framework.
- Whole-of-Government HRIS.
- Protective Security Policy Framework.
- Cyber Uplift Program.
- WoG Cyber Services.
- myService Tas.

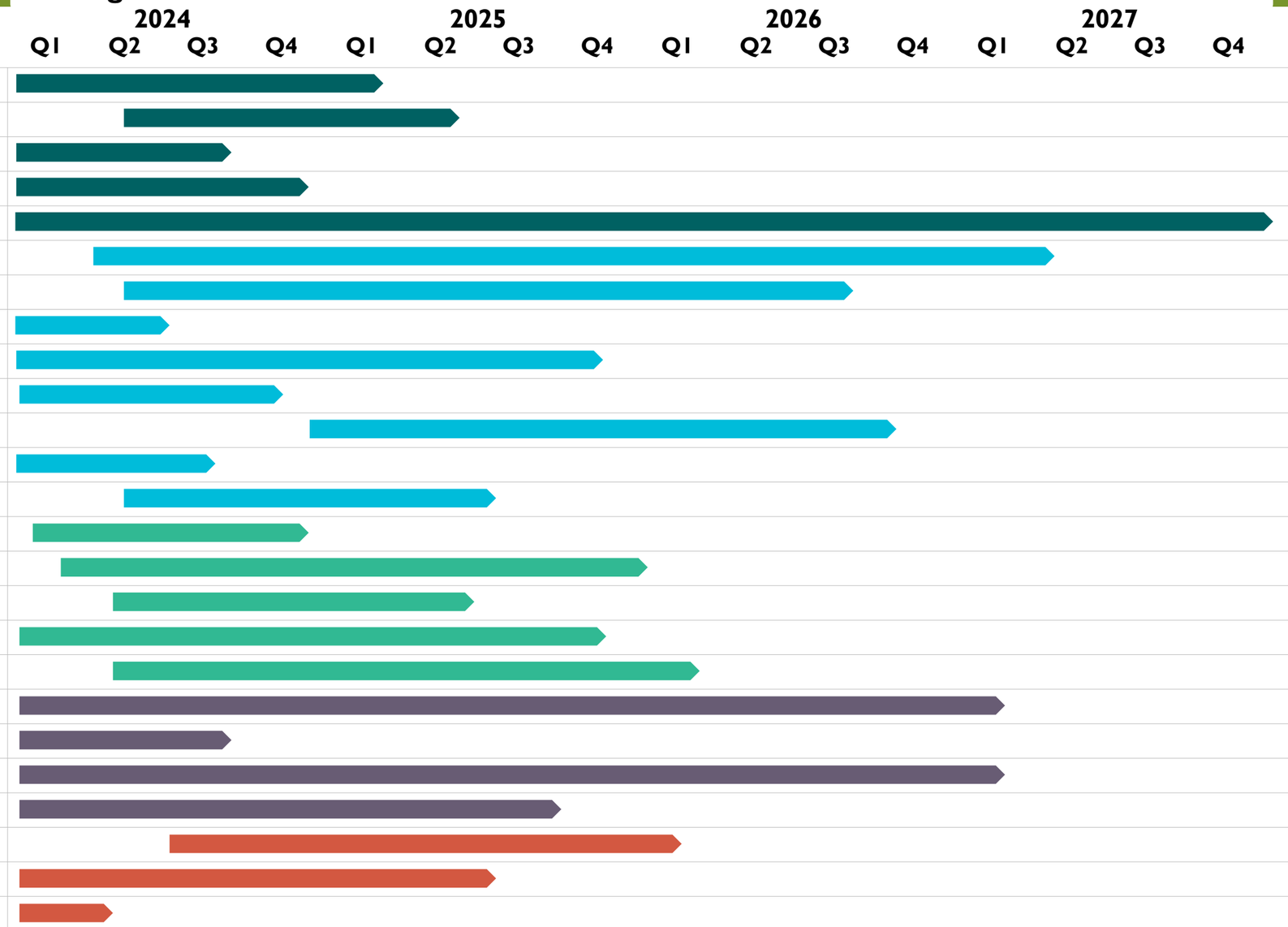
Digital & Data Services
Strategic Plan 2024 - 2027

PURPOSE: To Provide high-quality digital and data services to staff that will enable them to achieve the Department's strategic priorities and support them in delivering a sustainable Tasmania

Objective	Priority	How	Success
BUSINESS FIRST 	To understand our business processes and provide services to meet their diverse needs.	• Collaborating with Divisions and other agencies to provide the best service delivery options and align with divisional digital programs. • Develop the digital and data funding and investment model to deliver on the Department's strategic priorities and business as usual activities.	• > 90% SBU satisfaction for alignment of DDS strategy and SBU digital transformation. • Executive approved Digital and Data funding model.
SECURE & RELIABLE 	Protect the integrity of the Department's information and technology assets.	• Maintaining security by ensuring ICT systems and services remain resilient against growing cyber threats and changing security needs. • Enhance cyber-security awareness of Department employees and adopt a risk-based approach to managing cyber security.	• Each of the essential 8 assessment areas reach Maturity level 1 by Q2 2027. • All staff have completed mandatory cyber awareness training by August 2024.
FUTURE FOCUSED 	Lead the delivery of innovative services and solutions for the Department.	• Design processes and services to be flexible and scalable in order to adapt to changing business environments. • Trial new new technologies to learn and prepare the Department for adopting better, more efficient options.	• Adapt the NRE change framework and processes for DDS by Q4 2024. • Pilot a configurable reusable platform by Feb 2025.
SEAMLESS EXPERIENCE 	Equip our workforce to be productive, mobile, interoperable and secure.	• We will adopt a standardised approach to selection of business software solutions. • Increase staff mobility by enabling access to information from anywhere, at any time underpinned by a secure and reliable ICT infrastructure.	• DDSC Approved NRE Tas standard by Q1 2027 • > 75% staff satisfaction of technical capability to work remotely.
INFORMATION CULTURE 	Maximise the ability to make better decisions through information and insights to our business.	• Make information more accessible, easy to share and easier to find with information being digital by default. • Transform Agency data into insights, to enable better ways and better decisions.	• Implement a data and information management framework that has been approved by DDSC.

Digital & Data Services
Roadmap 2024 - 2027

Initiative	Timing	Link
Develop a digital and data funding & investment model		NRE Tas Strategy 6.5.3
Transition of Office of Racing Integrity		NRE Tas Strategy 6.4.4
Implement Jira Service Desk		NRE Tas Strategy 6.4.4
Provide input to SLAs for independent authorities		NRE Tas Strategy 6.5.3
Align SBU digital programs with DDS strategy		NRE Tas Strategy 6.4.4
Implement ACSC Maturity E8 Level 1 requirements		NRE Tas Strategy 6.6.3
Implementation of information PSPF actions		NRE Tas Strategy 6.6.3
Deploy Cyber-security awareness training for staff		NRE Tas Strategy 6.6.3
Completion of Information Asset register		NRE Tas Strategy 6.6.3
Assist with implementation of Container Refund Scheme		NRE Tas Strategy 2.2.4
Deploy Security Information and Event Management tools		NRE Tas Strategy 6.6.3
Develop a Cyber Incident response plan		NRE Tas Strategy 4.2.4
Replace the Reverse Proxy infrastructure		NRE Tas Strategy 6.6.3
Adapt the NRE change framework & processes for DDS		NRE Tas Strategy 6.4.2
Configurable reusable platform implemented		NRE Tas Strategy 6.6.2
Develop a Business case for a CRM		NRE Tas Strategy 6.6.2
Develop an evaluation process for new technologies		NRE Tas Strategy 6.6.2
Implement an AI policy for the Department		NRE Tas Strategy 6.6.2
Develop a standards approach for software procurement.		NRE Tas Strategy 6.6.2
Implement PC Rollout policy reflecting mobility capability		NRE Tas Strategy 6.5.3
Laptop fleet upgrade		NRE Tas Strategy 6.5.3
Digital Communication (phone) upgrade		NRE Tas Strategy 6.5.3
Develop a Data and Information management framework		NRE Tas Strategy 1.3.1
Implement data sharing infrastructure		NRE Tas Strategy 1.3.1
Deploy Food Score Card hosting infrastructure		NRE Tas Strategy 1.3.1



Digital and Data Services Business as Usual

Strategic Priority 6

Building a high performance department, driven by our people and our systems.

49 FTE 63 Staff
Infrastructure Services
Protective Security
System Services
Client and Engagement Services

250
Malicious emails blocked daily

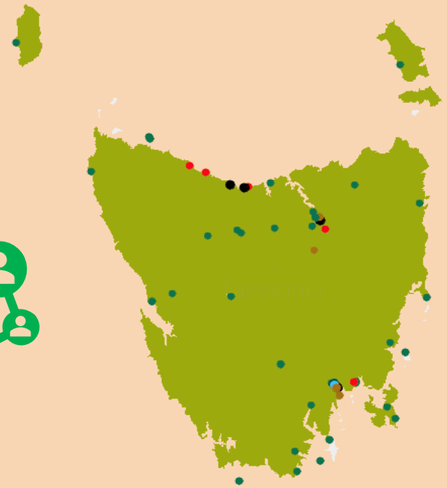
>23k
Service Desk calls per annum

1415 mobiles and tablets supported

2 Major Data Centres
3 Minor Data Centres

1696 Users
2200 Devices supported

24
Hosted Websites



75
networked sites
86
Staffed Sites

8
MOUs/SLAs

EPA FPA
PFT RTBG
Treasury WRR
AHT Service Tas

Strategic Priority 1

1.3 Enable business and employment through sustainable growth of Tasmania's industries.

7 Million
Records under management

1204
Peta bytes
Data storage

101
Databases

201
Business Applications

3500
Hard copy resources
3500
Digital resources

NOVEMBER 2024

IT Infrastructure Plan 2024 to 2029

Department for Education,
Children and Young People

Tasmanian Government

Table of Contents

Version 1.0 – 10/11/2024

Strategic context for IT Infrastructure in DECYP

The Department of Education, Young People and Children (the department) has a complex state-wide network supporting over 58,102 desktops, laptops, and tablet devices at over 300 locations around the state.

The IT Infrastructure and Business Application Solutions and associated business processes enable staff and clients of the department to be able to transact their business in a secure and safe environment from any location at any time with a minimum of disruption.

To facilitate the vision, this plan aims to move the department's IT Infrastructure and Business Application Solutions from a centralised network environment to one that utilises a high bandwidth network (maximising the potential offered by fibre connections particularly under the NBN), allowing central and cloud storage of data and business application solutions that enable department owned or student and client owned devices secure access to the resources they require to enable them to carry out their business anywhere, anytime.

To better support the rollout and adoption of additional technology systems, this plan also encourages the development of technology governance processes that provide clear accountability on technology selection and prioritisation decisions and ensures that new technology is strategically aligned and provides value to the department. The governance framework is not meant to prohibit or slow down new technology requests, but rather provide a streamlined pipeline for the various consultation and technology review processes that need to occur.

In broad terms the strategic directions of this IT Infrastructure and Business Application Solutions plan provides for the following key business and technical elements:

- Scalability – the ability to handle growth and cater for a Bring Your Own Technology (BYOT) device model in the client (students, library users) areas.
- Consolidation – the ability to bring together existing IT infrastructure and business application solutions to provide a more efficient IT environment.
- Agility and versatility – the ability to respond to changing business requirements and the changing technology landscape.
- Empowerment – enable business and service areas to readily adopt technology in a way that suites their needs, in platforms that are secure, managed, and reliable.
- Security –to provide the protection required to individuals, data, and business application solutions, based on alignment with the Australian Cyber Security Centre's (ACSC) Essential Eight maturity model.
- Safe – provision of online environments that promote and support safety and wellbeing while minimising the opportunity for children and young people to be harmed.
- Monitor – the ability to monitor in real time, either directly or via vendors, all elements of IT infrastructure and business application solutions to ensure they are working effectively.
- Availability – the ability to provide IT services continuously.
- Provisioning – the ability to provide required IT resources in a timely manner to the right users.
- Business Continuity –to provide continuation of service in the event of an incident that impacts the delivery of that service, and the ability to recover from an unexpected event and protect the department's data and information.

Underpinning all these elements is the need to deliver this in the most cost-effective way. The IT Infrastructure and Business Application Solutions plan addresses these requirements and can be broken down into various IT infrastructure categories with Business Application Solutions as an additional category.

1 End User Infrastructure

1.1 Desktop computers, Laptops, and tablets

The department has over 58,640 desktop, laptop, and tablet devices, with over 50,000 of these located within schools including teacher laptops. The desktop operating system for desktop and laptop computers is currently Windows 11. iPads run on the Apple iOS operating system. Software updates for these are centrally controlled and are provisioned as shortly after release as possible, once testing has been completed in the department environment. These computing devices are covered by four-year onsite warranty, throughout Tasmania including the Bass Strait islands.

Strategic Direction

The department has streamlined its preferred suppliers for desktop, laptop and tablet computers being Lenovo, Microsoft and Apple This has allowed us to focus on providing the best support model for our devices. Providing quick turnaround times on device security updates, driver updates and feature enhancements improves the devices usability and security.

Over the past 12 months we have updated most of our staff devices through our Computers for Teachers program and our non-school's device refresh programs. In 2024 there will be the addition of approximately 2500 devices deployed to Teacher Assistants and other school-based support staff.

Over the past five years we have seen an increasing number of teachers adopting highly portable devices in preference to the more traditional larger format laptops. To assist in this classroom transformation, increased options for lightweight devices to be deployed to the classroom environment to complement the direction in which our teachers are moving.

The deployment of Windows 11 at scale as part of the Computers for Teachers device rollout allows our users to access a raft of new features and modern business tools. Updating school devices used by learners and office administration staff, as well as those used by non-school users allows all department users to be on the same platform which enhances collaborative working.

Replacement Cycle

The desktop, laptop and tablet computers are replaced in a four-to-five-year cycle.

The department supports a Bring Your Own Technology (BYOT) model for students on a school-by-school basis to cater for their local circumstances. BYOT is a supplementary service at the school to support a minimum of one school-owned computing device for every three students at the school.

Business and service delivery units (Corporate Sites) BCN 855	2024/25 Devices Replaced	2025/26 Devices Replaced	2026/27 Devices Replaced	2027/28 Devices Replaced	2028/29 Devices Replaced	Totals
Facilities Management (1)	5	3	2	4	1	15
Non-school based staff	303	52	69	715	1,706	2,845
Libraries – staff	137	7	11	15	30	200
Libraries – Public Access	182	37	5	21	31	276
Total	**627**	**99**	**87**	**755**	**1,768**	**3,336**

School Sites BCN 823	2024/25 Devices Replaced	2025/26 Devices Replaced	2026/27 Devices Replaced	2027/28 Devices Replaced	2028/29 Devices Replaced	Totals
Teachers Award (Computers for Teachers)	30	30	30	30	5,463	5,583
School Support Staff (2)	2,100	300	600	30	30	3,060
SBM / Admin Staff	0	0	680	0	0	680
Facilities Management (1)	68	19	33	17	8	145
Student Devices Year 11 and 12 Extension Schools	0	1,000	0	0	0	1,000
Student Loan Devices (Digital Inclusion Action Plan)	0	0	1,000	0	0	1,000
Total	**2,198**	**1,349**	**2,343**	**77**	**5,501**	**11,468**

School Sites (SRP Funded)	2024/25 Devices Replaced	2025/26 Devices Replaced	2026/27 Devices Replaced	2027/28 Devices Replaced	2028/29 Devices Replaced	Totals
Student (3)	3,393	9,833	8,550	6,914	11,857	40,547
Total	**3,393**	**9,833**	**8,550**	**6,914**	**11,857**	**40,547**

Table 1 - End User Device replacement programs.

Note (1): Facilities Management device are devices that are not assigned to a staff member, that are provided by ITS and need to be replaced as part of our refresh cycle. They include such roles as:-

- Room controller, CCTV, building management, Telstra caching box

Note (2): Support staff is 3,000 staff members.

Note (3): Student devices are funded by individual schools via their SRP.

There are four device replacement programs that staff members can be assigned a device against, they are: -

- Non-school based staff – this covers all staff based in corporate offices, Libraries TAS, CFLC, ARL, etc.

For school-based staff there are three options

- Teacher award – all staff on the teacher award
- Admin staff – this includes SBM's and school admin staff
- Support staff – this includes teachers assistants

Staff should be assigned to one of these groups and allocated a device from within that pool. When staff have multiple roles, they will be assigned to the highest group they are a member of in the order of Teaching Staff – Admin staff – Support staff.

1.2 Software - Standard Operating Environment (SOE) managed by Intune

The desktop, laptop, and tablet standard operating environment SOE contains the base software installed on all desktop and laptop computers including Microsoft Windows operating system, Microsoft Endpoint Protection (anti virus / anti SPAM) and Microsoft 365 Office suite. The software licences for the SOE are coordinated and managed by ITS for all desktop, laptop and tablet computers owned by the department.

The device management for department devices, including Apple, was migrated to Microsoft Intune to modernise device management and standardise management of all operating systems in one platform.

Strategic Direction

Utilise an 'evergreen' release cycle where both feature and security updates are continuously released, optimising managing, updating, securing, and patching the operating system and SOE software applications.

- Optimisation of Intune Configuration: Fine-tune the configuration of Intune to align with the organisation's specific requirements and workflows. This includes setting up policies for security, application deployment, and compliance.
- Integration with existing systems: Integrate Intune with other existing systems and tools within the organisation's IT infrastructure to streamline processes and enhance efficiency. This could involve integrating with identity management systems, asset management tools, and service desk ticketing systems.

- Regular Monitoring and Maintenance: Improve monitoring strategy to ensure the smooth operation of Intune and department devices.
- Regularly review device compliance, security posture, and performance metrics to identify any issues or areas for improvement. We are looking at better ways to protect students using department devices on non-departmental networks this includes web filtering.

Replacement Cycle

Software is maintained, in most instances, in an evergreen state, with licences renewed yearly or as per their contract terms. Most software follows a regular (monthly, quarterly or annual) update patch cycle that both allows department staff to use the latest features as they are released as well as providing best practices for cyber security.

1.3 Printers and Multi-function devices

There are over 2100 printers of various makes and models located throughout the department including schools.

Over the past few years, the number of printers has dropped in schools and business units in favour of using multi-function devices (over 1000), which have print, scan and photocopy capability. These devices offer black and white and colour production. The department has preferred supplier(s) for multi-function devices being Ricoh and Konica Minolta.

To support a ‘follow me print’ function allowing employees to print at any location, the department utilises PaperCut MF software. There are currently two versions in use, a central cloud version and a local site version in some schools.

Where a multifunction device is not required a HP Desktop printer is utilised.

Strategic Direction

As business unit output requirements change or printers / multi-function devices require replacing, a review of the printer / copier requirements for the school and business area will be undertaken and from this a replacement strategy including replacement cycles will be developed for the individual school or business unit.

The preferences in developing this replacement strategy are:

- To lease, rather than purchase, multi-function devices.
- To minimise the use of desktop printers in favour of multi-function devices due to lower total cost of ownership.

To migrate all PaperCut local site versions from schools to the single central cloud version which will increase output options, while reduce management overhead of multiple versions and costs.

Replacement Cycle

Dependent on an individual school or business unit requirements as per their printer and multi-function device strategy. See the table below of current printer/multifunction device types.

Printers / Multi-Function Devices (Copiers)	HP	Ricoh	Konica Minolta	Other	Totals
Business and service delivery units	81	57	107	33	278
School	702	806	218	50	1,776

Table 2 – Printers and MFD types.

1.4 IT Support Costs

ITS has a mix of central IT staff and on-site IT staff. Central staff look after all central IT infrastructure located on-premises in the Government data centres, cloud hosted, and IT infrastructure distributed throughout business and service delivery units office and Library locations.

On site IT support in schools is allocated to schools on a ratio of the higher of department owned devices at the school or student FTE in the school, against the total state-wide IT school support staff number, with additional support provided by a central IT Helpdesk.

The IT Trainees located in schools are funded by the school via their annual School Resource Package, with all other IT Trainees positions supporting business and service delivery units locations funded in the central ITS budget.

2 Local Area Network

2.1 Local area network switches

Local Area Networks (LANs) are comprised of several distinct components - cabling (patch panels and communication cabinets), network devices (switches and wireless access points) and licensing. The department has standardised on Cisco for its networking hardware fleet. The licensing element of the network enables corresponding management solutions to be utilised to leverage return on investment and provide management of the equipment and other functionality (see 3.3 below).

Strategic Direction

Continuously review and update the department's Data Cabling Standards with the requirement that these must be referenced and adhered to for all building works and installations. ITS works closely with the department's Facility Services branch to ensure this occurs. All LAN cabling components must meet the department's Data Cabling Standards in all locations.

Asset data is collected and maintained as sites are upgraded, redeveloped, or built. Asset data reflects bandwidth, network devices, cabling specifications, racks, and other relevant configuration item (CI) information. All locations have Cisco network switches and wireless access points that support Whole of Government telephony services and identity-based access allowing both department and BYOT devices to be connected to the LAN.

- The Cisco network device fleet should remain current to avoid devices reaching end of vulnerability/security support periods thus enabling the deployment of scheduled software configuration updates to address vulnerabilities as they arise and maintain standard configuration across the networking equipment. Toolsets such as Cisco DNA-C can be utilised to manage and remediate the networking equipment in response to security vulnerabilities.
- Table 1 - End User Device replacement programs.
- Cisco networking equipment housed in the Government's Data Centres will be purchased with a Cisco 8x5x24 maintenance agreement for system failures. Failure of Cisco switches at all other sites will be addressed by either warranty or a backup supply of suitable spares.
- The Networking Tasmania LANaaS offering provides additional "value adds" or a catalogue of services in conjunction with the supply of networking equipment at Government shared office locations. This would consist of (but not be limited to) the availability of state-wide depots for the storage of switch hardware, pre-populating switches with modules and other components prior to deployment, delivery of switches to sites, storage of spares, hardware disposal, labelling of switches and provision of electronic serial numbers for switch hardware,.
- Continue to work with Telstra via the Networking Tasmania LANaaS agreement and Cisco on their new technology offerings, improvements, and network management toolsets with a view to evaluating these against business requirements and to assess technology stability within the department and Government network prior to wider deployment.

Replacement Cycle

LAN switches for business and service delivery units (Corporate) and School sites will be upgraded or replaced on a rolling 7-year cycle. This will be co-ordinated by IT Services. Licensing costs for operating systems should be included in the fleet renewal budget plan together with costs for ad hoc items (such as fibre modules) and planned minor cabling remediation works.

Business and service delivery units (Corporate Sites)	2024/25 Devices Replaced	2025/26 Devices Replaced	2026/27 Devices Replaced	2027/28 Devices Replaced	2028/29 Devices Replaced	2029/30 Devices Replaced	2030/31 Devices Replaced	Totals
2.1 Local Area Network (LAN) Switches	21	12	39	69	29	14	10	194

School Sites	2024/25 Devices Replaced	2025/26 Devices Replaced	2026/27 Devices Replaced	2027/28 Devices Replaced	2028/29 Devices Replaced	2029/30 Devices Replaced	2030/31 Devices Replaced	Totals
2.1 Local Area Network (LAN) Switches	261	270	239	204	234	243	249	1,700

Table 3 - LAN Hardware replaced on a rolling 7-year cycle.

2.2 Local Area Network cabling

The departments' Local Area Network (LAN) cabling is extensive and wide-ranging across many locations and buildings throughout the state. There is often a direct relationship between the age and condition of the building (or when it last had modifications) and the configuration and capacity of the cabling.

Strategic Direction

In conjunction with Facility Services and other parties, ITS have developed data cabling standards which are now included as requirements for all new building works.

The data cabling standards will be used as a reference point to ensure the LAN performs as expected and high-speed bandwidth is realised throughout the department's sites. The requirement for significant cabling or rack remediation works will be captured and provided to Facility Services based on remediation activities per site so that these can be included in the capital works budget. This will also include racks that require floor mounting to overcome potential safety and access issues.

Replacement Cycle

Cabling is reviewed and upgraded when building works are undertaken at the location and as part of remediation activities identified by ITS.

2.3 WIFI

The department's WIFI infrastructure is based on a Cisco solution provided by Telstra under the Networking Tasmania LANaaS agreement. This forms part of the whole of Tasmanian Government WIFI network enabling any Tasmanian public servant access from any location that has WIFI. This is largely managed by Telstra with level 1 support carried out by the department's IT support staff. The current fleet consists of over 5,800 Wireless Access Points (WAPs). To minimise client roaming issues at sites, locations are limited to a single model WAP wherever possible. Access to rich WIFI reporting and telemetry is limited in Telstra's shared environment with several portals providing WIFI information. Given this, most access points have now been transitioned to the

department's own DNAC platform so the benefits of richer telemetry data and reporting can be realised and a reduction in the number of management portals.

To date the criteria for the placement of WAPs has been one WAP per GLA (General Learning Area). In some cases, this has created problems, due to an oversaturation of WIFI resulting in excessive noise and interference. Additionally, it may not be the most cost-effective approach. WIFI site surveys should be undertaken as required to assist with optimal placement of WAPs as learning spaces and classrooms are re-designed and greenfield sites are established, or where sites report issues with WIFI coverage and throughput.

Strategic Direction

Regular review the availability of next generation WAPs and WIFI technology offered by Cisco including their Meraki WIFI products (e.g. 802.11ax and WIFI 6) with a view to continuously improving the end user experience. Current Cisco model WAPs offer compatibility with Meraki management systems which will provide future flexibility if the department chooses to move to a Meraki Cloud Management platform. To ensure optimum placement of WAPs in greenfield and redeveloped sites (and in locations where coverage issues are being experienced) site surveys will be conducted to determine optimum WAP placement and gain the best efficiencies from the WIFI fleet. Site surveys will also occur where sitewide WAP refreshes are taking place. To enable future migration to Software Defined Access (SDA) and realise a richer telemetry/reporting experience and improved operational management, the department has integrated its own DNA-C management portal instance.

The department's WAPs also support the new Whole of Government free public WIFI network in various corporate, Libraries Tasmania and other locations.

Replacement Cycle

WAPs for business and service delivery units, Corporate and School sites will be upgraded or replaced on a rolling 7year cycle. Licensing costs for operating systems should be included in the fleet renewal budget plan together with costs for associated required cabling as per the data cabling standards.

Business and service delivery units (Corporate Sites)	2024/25 Devices Replaced	2025/26 Devices Replaced	2026/27 Devices Replaced	2027/28 Devices Replaced	2028/29 Devices Replaced	2029/30 Devices Replaced	2030/31 Devices Replaced	Totals
2.3 Local Area Network (LAN) WAP's	41	76	76	76	76	76	76	497

School Sites	2024/25 Devices Replaced	2025/26 Devices Replaced	2026/27 Devices Replaced	2027/28 Devices Replaced	2028/29 Devices Replaced	2029/30 Devices Replaced	2030/31 Devices Replaced	Totals
2.3 Local Area Network (LAN) WAP's	1,024	719	719	719	719	719	719	5,338

Table 4 – Wifi Hardware replaced on a rolling 7year cycle

2.4 Network Monitoring, Management and Access

2.4.1 Network Management Tools, Network Access Control, and Internet Based Networking

Traditional network management toolsets are required to implement, manage, and control access to networks. Software defined access (SDA) now enables management, provisioning, and segmentation of the network fabric. In this context, access to the network is based on policy and identity rather than traditional Access Control Lists (ACLs) and Virtual Local Area Network (VLANs).

DNA-C (Digital Network Architecture Centre) and ISE (Identity Services Engine) are pre-requisites for SDA. DCNM (Data Centre Network Manager) is currently used to manage and monitor the Data Centre network switch fleet. Reporting and licensing is provided as part of Cisco hardware purchases.

Strategic Direction

Continue to consolidate Network management toolsets where possible and feasible. Work with DSS and Telstra in providing greater access, visibility and co-management options for government shared network management and monitoring systems. Evaluate new network management systems and technologies as they become available to assess their suitability for the department's network environment.

Undertake a review to establish and reconfirm the requirement for Software Defined Access (SDA) in light of technologies such as Direct Internet Access which shift network traffic directly to the internet.

Pending the outcome of the SDA review, conduct a proof of concept for SDA with the objective of removing the requirement for ACLs and VLANs. Access to the network is based on identity resulting in increased performance and security. It is anticipated that there would be ongoing costs associated with the procurement and ongoing licensing of Identity Services Engine (ISE) and this cost needs to be ascertained during the proof of concept.

Replacement Cycle

Implement upgrades or new network management systems and technologies as they become available.

2.4.2 Network Monitoring Tools and Logs

Monitoring toolsets including Security Information and Event Management (SIEM) solutions (e.g. Azure/Log Analytics) are used across the LAN, Data Centre and Wide Area Network environments. Appropriate toolsets can reduce management overheads significantly and leverage return on investment of existing network hardware infrastructure. They enable proactivity and an assurance that the network and related systems are operating optimally by providing increased visibility into the network. They also become increasingly important as on-premise Networks extend to the cloud.

Supporting toolsets can give visibility of communication between segments and applications, cyber threat intelligence feeds, baselines, indications of compromise, malware protection, logging, graphing, etc. Grafana is currently being used as a monitoring toolset. Log Analytics captures proxy logs, firewall logs, Netflow data, switch availability data and interface performance metrics. Many of these are critical log datasets from a regulatory and cybersecurity perspective.

Strategic Direction

The ongoing use of Azure/Log Analytics together with the centralisation of critical IT environment datasets should continue to form part of the department's strategic direction to facilitate single-pane-of-glass monitoring and reporting particularly as it relates to SIEM and cyber incident response. Other network monitoring solutions and management systems should continue to be evaluated as they become available to assess their suitability. These include toolsets which integrate with the department's Cisco technology fleet and provide monitoring and visibility of on-premise Networks extending to cloud performance including path visualisation.

Replacement Cycle

In most cases, toolsets such as Data Centre Network Manager (DCNM), are supplied as part of our yearly network switch and associated licensing purchases. Consideration should also be given to the purchase of additional toolsets not bundled with existing licensing, and particularly those toolsets which address existing gaps in functionality.

3 Wide Area Network

3.1 Wide Area Network

The department's Wide Area Network (WAN) is managed under the Whole of Government Networking Tasmania III contract. Under the contract, Telstra provide network core services including core switching, internet access, content filtering and inspection, load balancing, domain

name and IP address management, network authentication and authorisation, message gateway services and remote access services.

Telstra together with 42-24 and Field Services Group (FSG) provide approximately 330 connection services (WAN services) to the department under the contract. Department sites include schools, learning service and corporate offices, libraries, online access centres, child and family centres, youth justice and children and family services and shared (multi-department) sites. The three providers offer a range of WAN services including NBN enterprise and business grade services over various technologies. Network traffic at all department sites securely traverses the Network Core. Site connectivity, particularly at NBN fixed wireless sites, is complimented with a 4G failover service to provide a rudimentary level of redundancy.

Challenges continue to remain with limited-service offerings in remote locations throughout the State which often do not allow the use of higher speed fibre based connection services.

Internet access in the Network Core is provided by a 10 Gbps Telstra Internet Direct (TID) link dedicated solely for department use.

As WAN services are upgraded and speeds increase as they become available at locations throughout the state, congestion, and bottlenecks both at the local network level and within the network core are becoming increasingly common. This is particularly evident at times of high network usage which can be triggered by major events, e.g. Olympic Games.

Connectivity to resources hosted in Azure from on-premise is provided by a Microsoft ExpressRoute circuit provided by FSG.

Strategic Direction

In August 2022, DSS undertook a RFT seeking responses from vendors so that a new Data and Internet Services panel could be established and used by Tasmanian Government departments. Access to the new Data and Internet Services panel is now available (with Telstra services to be included by 3rd quarter 2024). New technologies include Low Earth Orbit (eg Starlink type) satellite services and discounted WAN services.

- Continue to work with DSS and network core and connection services panel providers to implement a Secure Access Service Edge (SASE) model incorporating SD-WAN technology to department sites. This will address WAN congestion at sites and within the Network core. It will also enable redundancy for sites by providing multiple WAN services and better visibility and control of network traffic ensuring WAN business continuity for essential business applications.
- Review and upgrade WAN services and technologies (e.g. Satellite technologies) to meet established minimum bandwidth requirements and provide an alternative to the sole reliance upon NBN Fixed Wireless. The increase in bandwidth capacity and options will also enable the adoption of a serverless IT infrastructure model in Schools removing IT infrastructure from the local site while improving service access.
- Continue to review network and cloud transit architecture (i.e. SD-WAN OnRamp and Azure Virtual WAN, etc). This can complement and/or reduce the reliance on the department's ExpressRoute service.

Replacement Cycle

The Networking Tasmania contract is broken down into several sub-parts covering the various elements of the WAN and internet access, with each of these sub-parts having different review / renewal periods. The department needs to maximise the benefits and flexibility offered by the Networking Tasmania contract and take advantage of rapid technology changes.

Review service availability options and costs annually with a view to seeking continuous improvements to availability, reliability, failover and throughput and to ensure Quality of Service for essential business services, and business applications solutions. This should include reviewing the department's internet bandwidth requirements and providers.

WAN Speed	NBN Fixed Wireless 50/10 Mbps	NBN 50/20 Mbps	NBN 100/40 Mbps	NBN 100/100 Mbps	NBN >100/100 Mbps	SD WAN Enabled Sites
Primary and Kindergartens	9	0	20	27	37	6
Secondary	0	0	3	1	15	1
Combined	4	0	1	4	6	1
Senior Secondary	0	0	0	0	2	0
Special/Outreach	0	0	6	0	3	0
Corporate including Libraries Tasmania	6	1	28	5	16	2
Total	**19**	**1**	**58**	**37**	**79**	**10**

Table 5 - National Broadband Network (NBN) - Summary of Connections

WAN Speed	10 Mbps	20 Mbps	50 Mbps	100 Mbps	>100 Mbps
Primary and Kindergartens	1	0	1	27	6
Secondary	0	0	0	5	9
Combined	0	0	1	13	1
Senior Secondary	0	0	0	1	6
Special/Outreach	1	1	0	3	0
Corporate including Libraries Tasmania	0	5	1	11	11
Total	**2**	**6**	**3**	**68**	**33**

Table 6 - Other WAN services – Summary of Connections

3.2 Remote Access

Remote access is the ability to gain access to the department's IT services and business application solutions from either outside the department or from a location within the department that is not considered an individual's "base location". This includes staff at non-department locations, telecommuters / mobile users (e.g. between sites) and those who are travelling interstate and overseas who may require access to the department's IT services and business application solutions. In addition to this, client groups such as teachers and students requiring access to learning management systems from their home to access classroom resources. Remote access for department staff devices is currently provided by an "always on" Cisco AnyConnect VPN Client installed to the device.

All department IT services including business application solutions will be geo-blocked so that by default they can only be accessed from within Australia and business and service delivery units will need to justify where they should be available in other broader locations.

Staff will be able to request overseas access to services like email on a case-by-case basis when they undertake work related travel.

Strategic Direction

Technologies such as Microsoft 365 and cloud hosted learning management systems enable access from a greater range of locations, thus the need for a traditional remote access solution is diminishing. The emergence of cloud remote access technologies such as Azure Virtual Desktop and Application Proxy enable access to internal department resources for staff and students. Cloud based authorisation and authentication technologies, i.e. conditional access, geo-blocking and multi factor authentication (MFA) will be essential in the provision of secure access to department IT services and business application solutions.

As part of the WoTG Networking Tasmania Core Agreement contract renewal with a focus on Secure Access Service Edge (SASE) the department should seek to adopt a Zero Trust Network Access model to improve our cyber security posture and provision of IT services to users.

Replacement Cycle

Continue to advocate for the department's remote access requirements for inclusion in the whole of government (WoTG) Networking Tasmania contracts.

As business application solutions are upgraded or modernised, remote access and authentication will be reviewed in line with contemporary policies and practices.

4 Infrastructure

4.1 Cloud Platforms

Cloud platforms provide a convenient mechanism to out-source parts of the infrastructure and application stack which reduces onboarding and development cost for new technology solutions. Broadly these service levels are Software-as-a-Service (SaaS; the entire application environment is out sourced), Platform-as-a-Service (PaaS; the computing and data environment is outsourced,

but the application needs to be developed) and Infrastructure as a Service (IaaS; only the physical infrastructure and networking is outsourced).

Tasmanian Government have had a cloud-first policy for new technology since 2017 which the department have been following since it was released. Our current preferred cloud platform is Microsoft Azure, as it offers synergy with existing technology services that we depend on (identity and Microsoft 365 office software), and offers a range of services that provide a clean migration path for legacy on-premise business application solutions hosted in Tasmanian datacentres. Currently around 70% of department application workloads are hosted on cloud platforms (IaaS, PaaS or SaaS).

As outlined in the servers/compute and application sections, the current strategy for individual workloads is to invest in solutions as high up the stack as possible (e.g. preference SaaS over PaaS, and PaaS over IaaS) as they are typically more cost-effective compared to IaaS. The service level selected will depend on the flexibility of the technology and the consumers of the system - our preference is to follow an 'adopt over adapt mantra whereby (whenever possible) business processes are changed to suite business application solutions available on the market, instead of developing software to match current business practices which are very bespoke and may no longer be contemporary. The assumption is our department is not unique and that we should be able to capitalise on investments in other sectors to reduce our system development cost, leverage business application solutions that are already developed and in use in other government departments or businesses and reduce technical debt that ultimately complicates application lifecycle management and increases the departments cyber risk profile.

Whilst cloud offers significant development benefits, it does increase operational costs as services are charged on a subscription basis rather once-off capital expense. As such there is a need to drive some cost efficiency in our cloud platforms to prevent run-away consumption increases as we move more services to cloud. Achieving this will require a combination of generating competitive pressure on cloud providers (through competitive procurement processes and contract negotiation) and adoption of shared, single-instance cloud platforms (e.g. Data Lake) whenever suited to drive service efficiency. At a technology level, our new development standards also require bespoke development to be completed in a provider-agnostic way (leveraging containerisation) which will provide an exit strategy for the department should Microsoft Azure not remain cost effective into the future.

At a staff level, we are aware that across the department there is often a view that cloud is "insecure". Industry studies have highlighted that a properly managed public cloud platform is often more secure than traditional on-premise IT hosting due to higher level of regulatory compliance reached by providers like Microsoft, and their orders-of-magnitude higher investment in cyber security funding when compared to Tasmanian Government. They also manage their services 24x7 compared to a traditional work day that most government departments use. The risk areas are around incorrectly configured platforms, and SaaS vendors that do not have the organisational maturity to adequately secure their cloud infrastructure. To manage these risks, we have developed several cyber risk assessment processes that are being applied rigorously to new product selection, and we are routinely undertaking risk and operational readiness assessments with independent parties to ensure our cloud platforms remain secure and aligned to best practice.

4.2 Servers – physical and logical

Central servers are largely virtual hosts. These servers are clustered with many virtual servers deployed to each cluster. This maximises the efficiency of server computing hardware and reduces the number of physical servers required. Current trends are to move workloads further up the technology stack to cloud-based Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), reducing the need for on-premises physical servers which are mostly housed in the Tasmanian Government data centres.

The department's physical infrastructure supporting the virtual hosting environment has passed seven years in age and is rapidly approaching end of life. The expectation is this hardware will need to be retired in the coming twelve months. Whilst significant progress has been made in moving virtual machines to cloud-based Infrastructure-as-a-Service (IaaS), the current strategy of modernising underlying platforms and opportunistically moving to Platform-as-a-Service and Software-as-a-Service requires significant planning and time and resource investment from business application solution owners. Additionally, a bulk lift and shift has been largely unsuccessful to date due to complexity. As such, ITS has adopted a combination of various approaches in moving off the ageing physical server infrastructure. These include deep analysis activities to identify servers that can be decommissioned, lift and shift of some workload and modernisation of other workload. Hardware support has been extended together with provision of extended security updates. The expectation is that the Department will have minimal business application solutions hosted in government-managed datacentres by end-2024.

For Infrastructure-as-a-Service workloads the department leverages two cloud providers. Tasmanian based Field Services Group (FSG) IaaS offering and Microsoft Azure Private Cloud IaaS. Azure Private Cloud IaaS has been found to be more scalable and cost-effective compared to FSG IaaS, whilst providing a range of value-add features that streamline integration with other cloud services such as Microsoft365. As such ITS are planning to consolidate FSG IaaS into Azure IaaS within the next five years after exiting government-managed datacentres.

Previously Azure IaaS has been procured through a Cloud Service Partner (CSP) arrangement with FSG. The CSP approach was adopted to meet requirements outlined in the original Tasmanian Government Cloud-First policy. This policy has since changed, and ITS believe the CSP arrangement exposes the department to additional cybersecurity risks and may inhibit a 'value-for-money' approach to Cloud Services by preventing the department from leveraging cost saving capabilities in Private cloud. As such ITS are intending to consolidate all Azure IaaS workloads onto a native Microsoft Enterprise Agreement subscription in alignment with existing PaaS services.

Schools are provided with a single Infrastructure Server (funded centrally) to host file shares, printers, authentication/authorisation at a local site level. With a move to Software-as-a-Service for many School-based IT Services (Microsoft Office365, email, file shares through OneDrive/Teams, on-line learning through Canvas) the requirement for local server infrastructure is diminishing. It is envisioned that several services currently hosted on physical servers will be decoupled as services like DHCP are transferred further upstream.

Whilst uptake of Microsoft365 at a school-level has increased in the last three to five years, there are still several challenges around staff training / general change management preventing widespread adoption. Additionally, cloud services do not have an offering for latency-sensitive file editing such as multimedia editing performed at some schools via the Adobe toolsets as part of

student learning programs, or for local site-based building management software. Given these challenges it is expected that some schools will need some form of local file storage capability for the next three to five years.

Strategic Direction

- Procure new workloads as far up the technology stack as possible: SaaS, followed by PaaS, private cloud IaaS, then Whole of Government IaaS, as per Tasmanian Government Cloud Policy.
- Consider opportunities to modernise existing business application solutions and take advantage of IaaS, PaaS, autoscale and geo-redundancy capabilities in private cloud.
- Continue to develop and formalise cloud infrastructure standards and reference architectures in conjunction with service providers and to provide clear guidance to software vendors on the use of cloud-based infrastructure.
- Utilise contemporary practices including Continuous Integration (CI) and Continuous Deployment (CD) to bring automation and robust processes to system deployment and maintenance. Continue to standardise on Terraform for automation given ease-of-use and support for other public clouds outside of Microsoft Azure.
- Where possible, remove dedicated Pre-Production and Development environments in favour of temporary cloned production environments and utilisation of CI / CD processes. Using CI / CD in this manner also serves as a cost management strategy for cloud and reduces infrastructure risk profile by reducing the number of permanent running environments.
- Continue to invest in training and awareness programs for ITS staff and departmental business systems staff to build understanding of contemporary, cloud-based technologies and ensure underlying assumptions about the security, reliability and suitability of cloud platforms are addressed.
- Opportunistically look to move school IT infrastructure to cloud-based solution whenever suitable. This may occur at a service/function level (e.g. move site backups to the cloud), or at a school-level dependent upon their bandwidth connection as a high speed fibre connection is preferred e.g. move several pilot schools to cloud-based infrastructure, test assumptions about suitability/performance, and leverage the pilot schools as demonstrators for the rest of department.

Replacement Cycle

- Reduce requirement for physical and virtual on-premise servers through adoption of SaaS, PaaS, and IaaS.
- Current on-premise server replacements (in schools in particular) will be considered where no alternative is available.
- Work with End Device team on Autopilot and Intune end user device software updates strategy to determine if on-site local servers for schools are required beyond 2026. Currently software distribution for end device patching / management is cached on local school servers.

Sites	2024/25 Devices Replaced	2025/26 Devices Replaced	2026/27 Devices Replaced	2027/28 Devices Replaced	2028/29 Devices Replaced	2029/30 Devices Replaced	2030/31 Devices Replaced	Totals
4.2 Servers	71	0	0	0	0	0	0	71

Table 7 – Physical Servers

4.3 Server Operating Systems (OS)

An operating system (OS) is the software component of a server computer system that is responsible for the management and coordination of activities and the sharing of the resources of the server. The operating system acts as a host for business application programs that are run on the server. The department currently uses a variety of operating systems on its 800 servers located at over 250 locations. A portion of these are physical local site servers at school and remote business unit locations state-wide, whilst others are virtualised. Several servers are hosted in Tasmanian government data centres and host business specific business application solutions.

As services transition to contemporary cloud-based technologies such as Platform/Software-as-a-Service the operating system will become less of a concern given the OS is only pertinent for IaaS and on-premise services.

Current business application solution deployment processes on IaaS/on-premise services are highly dependent on Operating System version which leads to lifecycle management issues when the OS reaches end-of-support from Microsoft and the business application solution is still required, ultimately increasing the cyber security risk as key business application solutions are running on unpatched platforms. Effort needs to be made to decouple application dependence on server / operating system infrastructure to minimise this risk and the operational burden on IT support staff to manage them.

Strategic Direction

- During system lifecycle processes, upgrade to Windows Server 2022 which is a long-term operating system that provide five years of mainstream support and five years of extended support.
- For new systems that are unable to move to PaaS/SaaS environments, mandate automated deployment processes (preferably through CI/CD) so that the systems can be easily deployed to new infrastructure when the OS reaches end of support.
- During future procurements of new business application solutions clarify OS supportability with vendors / providers so that the upgrade path is understood (e.g. will they support current –1 operating systems).
- Continue to invest in automation capabilities for business application solution deployment and application configuration. Automation is a key to enabling cloud practices such as automatic performance scaling to meet workload / demand, continuous integration and enable deployment, and automated system lifecycle management, all of which will reduce IT

operational overheads, lower time to resolution for support issues and improve overall cyber security posture and service efficiency.

- Work with others to improve processes and policies to better facilitate wholistic lifecycle management of business application solutions. These include, but are not limited to, PaaS offerings, Windows server operating systems, database engines, .NET versions and application versions.
- Utilise the managed service provided by Patterson Brown to support legacy Solaris and Linux systems whilst progressing the migration of some of those systems to Azure IaaS/PaaS where possible, e.g. Library systems (Symphony).

Replacement Cycle

The department still has a significant number of servers running on legacy operating systems. From a support and maintenance perspective it is important that these legacy servers are actively replaced with more contemporary versions. Legacy operating systems versions increase risks, as the ability to resolve technical issues diminishes and the risk of security issues increases as the vendors develop the newer versions of the OS but don't provide the same levels of patches and updates to older versions of the OS.

The difficulty in upgrading to a new version of the OS can however be the dependencies that exist between a business application solution, and it's supported OS.

To mitigate this risk in the interim, ITS have applied extended security updates (ESU) to the Microsoft 2012 R2 Server fleet.

4.4 Infrastructure – Storage

Storage (including backup and recovery)

In the department's business units and service delivery unit areas, ITS have consolidated server disk storage to large Storage Area Networks (SANs) hosted in the Tasmanian Government data centres. These SANs are now aging and the need for replacement is diminishing due to the uptake of technologies further up the stack (SaaS, PaaS, IaaS). As with physical datacentre servers, the expectation is this hardware will need to be retired in the next 12 months, and as mentioned previously, the department is adopting a multi-faceted approach identifying those applications, servers and systems that can be decommissioned, migrated, modernised, etc.

Schools still utilise the traditional model of site-based local servers and storage however with recent investments in improved WAN services (bandwidth and redundant links) there is an opportunity to move some services to cloud-based solutions such as Microsoft365 and Canvas over the next three to five years. Some schools will still require local storage to support latency-sensitive workloads such as multimedia editing via the Adobe toolsets as part of student learning programs where cloud-based solutions are not yet fit for purpose. To protect the data stored at local sites, each School has a NAS (Network Attached Storage).

Strategic Direction

- Reduce the requirement for central storage through adoption of SaaS, PaaS and IaaS and private cloud services.
- Continue to increase bandwidth to schools whilst improving link resiliency via secondary backup WAN services to reduce requirement for local storage solutions.
- Transition existing backup services to cloud-based technologies where appropriate – initially looking to replace onsite NAS backups and offline/off-site USB backups in schools with an Azure-based solution.

Preference cloud-based solutions in schools for user data – e.g. Microsoft OneDrive for Business and Teams/SharePoint over local storage on school servers. This will continue to be a focus of discussions and actions between Teaching and Learning, Learning Services, and IT Services over the next couple of years.

Replacement Cycle

Maintain SAN based storage centrally to support legacy workloads until applications are migrated to SaaS, PaaS, IaaS, or public cloud services.

Core storage infrastructure is replaced every five years where a cloud service offering can't be utilised. On-premise storage infrastructure is upgraded / increased as necessitated by the requirements of department Business Application Solutions.

Maintain infrastructure in schools until bandwidth enables schools to only use cloud-based solutions for storage.

Migrate school backup solutions to the cloud as part of the school server refresh.

4.5 Infrastructure – Data Platforms

Databases

A database is a collection of data that is organized so that it can easily be accessed, managed, and updated. Most database technologies used by the Department are based on Microsoft SQL, with a small footprint in Oracle (library systems) and MySQL/Postgres Platform-as-a-Service for WordPress hosting.

ITS have started to leverage contemporary cloud-based PaaS databases hosted out of Microsoft Azure private cloud for new services, but have found that these offerings don't have full feature parity with traditional full-stack SQL offerings and hence are not a direct replacement for established business application solution databases.

Outside of traditional relational database management systems (RDBMS) the department have invested in a contemporary data lake architecture hosted in Azure. The Data Lake is used as a support for business intelligence reporting and orchestrating data movements between systems (as per the department's data integration standard). The Data Lake provides several benefits compared to traditional warehousing architectures including reduced cost to onboard new datasets, a more flexible data sharing architecture (that allows sharing data externally), support for both structured, semi-structured and unstructured data and improved analytics capabilities including native support for machine learning and artificial intelligence.. The expectation is the Data

Lake will eventually replace traditional Data Warehousing for the department over the next three to five years.

The continued uptake of structured data systems and the increased number of technology solutions has highlighted several data governance challenges for the department (similar to other government entities). Data governance refers to the internal standards and policy framework that dictates how data is gathered, stored, consumed and disposed across the department. Given the volume of databases across the department (over 3,000), there is a need for a policy framework and data catalogue that aggregates domain knowledge and captures information and data risk classification for the departments databases. IT Services are supporting the Data, Systems and Insights (DSI) team in the development of the policy work and have identified Microsoft Azure Purview as a technology solution to produce an automated, consolidated data catalogue to improve visibility of the departments data assets.

Strategic Direction

- Move system integration from traditional database level integration to REST APIs to facilitate further adoption of contemporary cloud-based solutions.
- Continue to invest in the Azure Data Lake as a centralised integration and reporting abstraction layer for business application solutions and associated departmental datasets.
- Continue to utilise contemporary versions of Microsoft SQL for IaaS consolidating the number of servers where possible and migrate databases from legacy versions of Microsoft SQL to contemporary versions.
- Actively decommission or migrate the few remaining Oracle based systems in partnership with the appropriate business unit as they renew / upgrade / replace the business application solution over the next two years.
- Continue to invest in the Data Lake architecture as a replacement for traditional data warehousing and opportunistically transition systems to reading from / writing to the Data Lake instead of the warehouse where required.
- Invest in organisational Data Governance practices including an Information Classification Scheme to ensure the enterprise data environment is appropriately managed and continues to add value to the department's reporting needs.
- Continue to invest in Microsoft Azure Purview as a technology solution to automate risk classification of department datasets and provide a consolidated data catalogue for department datasets.
- Utilise contractors for high level support of database environments due to their complex nature.

Replacement Cycle

Database lifecycle management closely aligns with business application solutions or services lifecycle. New business application solutions will be deployed utilising PaaS services, in turn reducing the requirement for on premises databases services.

The difficulty in upgrading to a new version of the database can however be the dependencies that exist between a business application solution and its supported database. Sometimes this dependency may mean that there is a need to upgrade to a newer database version than originally planned otherwise the upgrade cannot proceed or install a new business application solution.

Investing in CI/CD approaches for IT Infrastructure (as outlined earlier) and using application-to-application (i.e. API) integration techniques minimises the complexity of platform upgrade activities and will allow the department to be more agile with migration/upgrade activities in future.

4.6 Infrastructure - ICT Facilities

Facility Management and Hosting Services

The department broadly has two distinct IT facility management needs. These are the requirements of the main Hobart Whole of Tasmanian Government (WoTG) data centres and the requirements of other department satellite locations (schools, youth detention, learning service offices, libraries, online access centres, business unit locations, etc).

Strategic Direction

The department utilises two WoTG Data Centres currently for hosting on-premise IT infrastructure however we will seek to reduce the requirement for hosting workload within these data centres as previously mentioned. The two data centres are located at – Site A (42-24 Moonah) and Site B (42-24 Cambridge). It is envisioned that network and IT infrastructure management workloads will continue to be hosted within these data centres for some time.

- Continue to adopt Infrastructure as a Service (IaaS) via Microsoft Azure services both on-island through FSG and via Australian Microsoft data centres to reduce the requirement for local data centre services.
- Continue to adopt technology further up the stack to reduce requirement for data centre services. As part of any revised Whole of Government cloud policy, also implement other public cloud services.
- Undertake an audit of IT Server infrastructure and storage for sites, particularly schools, to inform a migration pathway for server infrastructure requirements including adoption of a serverless architecture where possible.
- Where possible migrate local site services from on premise local site server infrastructure to the cloud as WAN bandwidth and availability allows.
- Undertake a review of backup requirements at a holistic level as it applies to site data storage and the department as a whole.
- Replace UPS (uninterruptable power supplies) which support server and storage infrastructure at those sites where infrastructure will continue to exist and a full “serverless” model cannot be adopted. Further evaluate the requirement for the provision of UPS to support school office environments in the event of power failures.

Replacement Cycle

Continue to consume Networking Tasmania III WoTG Data Centre as a Service (DCaaS) during transition to cloud based services.

Reduce footprint in both department and DCaaS sites through consolidation and migration of services up the technology stack and into the private cloud where possible.

5 Infrastructure – Telephony and related services

5.1 Telephone Services

There are around 11,000 fixed lines located throughout the department including business and service delivery units, schools, libraries, and CFCs state-wide and 3,700 mobile services, with the majority of these located in schools.

Strategic Direction

All business and service delivery units areas migrated to Whole of Tasmanian Government VoIP (Cisco) in 2016 as part of the new Whole of Tasmanian Government VoIP contract. DSS is now undertaking a project to exit from this contract and offer up new services in line with modern work practices under a new Whole of Tasmanian Government panel arrangement that the department will need to procure off.

All schools currently use Small Sites VoIP (Samsung) solution under the Whole of Tasmanian Government VoIP contract. This system has now gone end of life and now needs to be replaced and is covered in the new Whole of Tasmanian Government panel arrangement that the department will need to procure off.

As we transition away from our current fixed-line telephony solutions for both school and non-school sites, DECYP in partnership with DSS will run an RFQ process looking for a strategic partner to design a telephony solution that will meet our needs for the next decade based upon the service offerings off the new Whole of Tasmanian Government panel arrangement.

Improved management of DECYP mobile phones and departmental data accessed via mobile phones will assist in improved data security and control for these devices.

Full management of a mobile device would be targeted at DECYP owned devices supplied to our users. This allows for a remote wipe of the device in the case of it being lost or stolen. It also allows for controlling web filtering and which applications can be installed on the phone. All departmental phones purchased since 2021 have been Intune enrolled which allows the device to be fully managed.

Mobile phones that are currently owned by DECYP that are not managed, will become managed when they are next replaced or will need to go through a factory reset to defaults (as if new) to have full management enabled on these devices.

In addition to managing the telephone device, there is an increased need to manage applications on the device via Mobile Application Management (MAM). This allows the department to control the data accessed by any MAM supported application. It allows the ability to remotely wipe the data and prevents copying of DECYP data outside the department. This level of management can also be applied to users personal mobile phone devices if they access DECYP data eg their DECYP email account. Whilst it allows for control of departmental data on the device, it does not affect the users personal data or their ability to use it for the personal tasks as they want.

ITS are trialling the use of MAM in anticipation of publishing a new Mobile Device Policy and Procedure which will prescribe the controls around device purchase, management, and usage

including when using personal devices to access DEVYP systems or data.

Replacement Cycle

Part of the whole of Tasmanian Government voice services contracts (there are several covering the various types of telephony services including carriage) and replacement cycles for each service type.

Mobile telephone handsets are replaced as required but normally on a minimum four year cycle.

The Samsung VoIP solution is end of life, and schools need to plan for their Samsung VoIP system replacement in their individual school IT Infrastructure plan based upon the options available under the new Whole of Tasmanian Government panel arrangement as they become available.

5.2 Video Conferencing (VC)

The department makes use of Microsoft Teams as its video conferencing / unified communications software platform. This is provided by Microsoft via its Microsoft 365 service and the annual Microsoft agreement licences all department staff for its use. Students are also covered by Microsoft Teams through Microsoft 365 as part of the department's Microsoft licence agreement.

The type of end device VC hardware required for video conferencing will depend on the use case from single users with personal VC equipment to larger units for use in classrooms or office meeting rooms.

The department's Learning Management System (Canvas) has a video conferencing function within its default configuration that is used by some schools to interact with their students.

Strategic Direction

Continue the use of Microsoft Teams as the software toolset to allow video conferences with external to government users, for administrative and educational purposes.

Use of modern Microsoft Teams Room equipment and Microsoft Surface Hubs as the hardware in any business and service delivery units meeting rooms to enable group video conferencing and collaboration to be undertaken, including with external stakeholders.

DECYP are undertaking a review process utilising industry experts to determine our future offerings in the video conference space. Microsoft have recently made fundamental changes to the Surface Hubs which has presented DECYP with an opportunity to review our current position and evaluate options in this space.

Staff continue to use personal video conferencing hardware attached to their standard department device or via the soft client software on their department mobile telephone.

In partnership with Teaching and Learning work with schools to develop various use cases of video conferencing to maximise its use including for educational learning purposes through access to Microsoft Teams in Microsoft 365, and the video conferencing component of Canvas.

The department are undertaking a review process utilising industry experts to determine our future offerings in the video conference space. Microsoft have recently made fundamental changes to the

Surface Hubs which has presented DECYP with an opportunity to review our current position and evaluate options in this space which will inform future directions for these VC use cases in future years.

Replacement Cycle

For the software component of Microsoft Teams based video conferencing solutions, the replacement cycles are enabled through Microsoft 365 evergreen processes which provide regular updates to the Teams software.

For VC hardware, continue to replace in line with device replacement cycles for personal equipment and a minimum of 5 years for room-based equipment.

The department will need to replace all Surface Hub version 1 devices before August 2025. The operating system on these devices will go end of life at this time and these devices cannot be upgraded.

Business and service delivery units	2024/25 Devices Replaced	2025/26 Devices Replaced	2026/27 Devices Replaced	2027/28 Devices Replaced	2028/29 Devices Replaced	Totals
5.2 Surface Hubs	67	7	1	26	26	127

Schools (funded via their SRP)	2024/25 Devices Replaced	2025/26 Devices Replaced	2026/27 Devices Replaced	2027/28 Devices Replaced	2028/29 Devices Replaced	Totals
5.2 Surface Hubs	4	2	1	1	3	11

Table 8 – SurfaceHub Video Conferencing equipment

6 Cyber Security

Cyber Security services

The Whole of Tasmanian Government Cyber Security Framework and associated policies, guidelines and play books are under development by the WoTG cyber security team of the Digital and Strategic Services (DSS) branch in DPAC. Currently there is an overarching government Cyber Security Policy supported by a subset of guidelines. Once further guidelines and playbooks are released, the department will review and tailor them to suit the specific context of the services provided by the department, at which point they will undergo a formal approval process with the department Executive Committee. This work will be undertaken during the 2024 and 2025 calendar years.

Currently there is limited cyber security services available at a WoTG level. In addition to the policies and guidelines, DSS aids with Cyber Security indecent response and external vulnerability scanning services. DSS have indicated that they are working towards increasing their Cyber

capability by running a program of works that includes incident management, baseline cyber awareness, enhanced workforce capability and extending vulnerability management, however this uplift in capability has been slow to materialise.

The department has migrated its Vulnerability Management managed service onto the DSS managed service. The department is also trialling a managed Security Operations Centre for out of hours monitoring. DSS have indicated that they are not currently considering a WoTG monitoring service, and the department expects to go to market at the conclusion of the current trial in 2025.

The department uses Microsoft Sentinel, which is a scalable, cloud-native solution that provides:

- Security information and event management (SIEM)
- Security orchestration, automation, and response (SOAR)

Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise. With Microsoft Sentinel, the department gets a single solution for attack detection, threat visibility, proactive hunting, and threat response.

IT Services reports to the department's Risk Management and Audit Committee (RiMAC) on information and cyber security areas in February, June and October. This includes a summary of IT cyber security key actions and improvements. IT Services is developing a Cyber Security uplift program to better meet, and report on adherence to the Australian Signals Directorate (ASD) Essential Eight framework and its associated maturity levels.

Following on from the cyber friendly phishing training that has previously been provided, IT services will utilise the free Fortinet cyber awareness and training materials to complement the baseline service offered by DSS. A major focus will be expanding existing cyber awareness beyond Phishing to encompass more aspects of good cyber hygiene such as device and software updating, data backup and the use of passphrases.

Business Operation Support Portfolio business units have placed an emphasis on the development of Business Continuity Plans (BCP). The methods and templates devised from this development can be utilised to assist other business units in developing BCPs in their context. ITS are also collaborating with other business units to create IT Recoverability Plans for each critical business applications identified during the business units BCP process.

The ICT Acceptable Use Policy is now provided electronically to all staff each day when logging into the department's network. A Telephone and data Acceptable Use Policy, addressing the use of mobile phones and data devices, has been developed and is currently in consultation before going to the Executive Committee for approval. There are also distinct ICT Acceptable Use Policies tailored for students based upon their year level and clients of Libraries Tasmania.

Strategic Direction

The overarching strategic direction is to adopt a modern security design philosophy in all new solution deployments, which embraces a Zero Trust strategy aimed at providing protection against current and emerging threats. This strategy is underpinned by alignment with the ASD Essential Eight framework, and more broadly the ASD Information Security Manual.

ITS Cyber Security Uplift

- Increase the department's cyber security posture through the implementation and enhancement of Privileged Access Management (PAM) and Privileged Identity Management (PIM) systems, underpinned by MyLogin as the core data set.
- Continue to improve and expand the SIEM and SOAR environment by automating responses to common events and alerts based upon prior learnings across government enhancing our ability to detect and mitigate threats in near real time.
- Implement effective, contemporary security controls that are aligned with the ASD Essential Eight framework by adopting a risk-based approach to prioritise and address vulnerabilities, threats and recommendations.
- Automate the process of creating and assigning device vulnerability remediation tasks discovered by Microsoft Defender.

Data Sharing Governance Uplift

- Review, document, assess and uplift the management and mechanisms of sharing data sharing with third parties.
- Continue the development of standards, procedures and playbooks to support the evolving cyber security governance requirements.

User Education

- Develop a Cyber Security education program focusing on best practices for individuals and the protection of data using a contemporary suite of cyber eLearning resources available to all department users.

WoTG Collaboration

- Continue to collaborate with DSS at a WoTG level to leverage WoTG initiatives with the aim to leverage economies of scale or provide greater capabilities to either the department or WoTG through shared resource use.

Replacement Cycle

Continual improvement of the security toolsets as the industry matures, with emphasis on automated detection, response and remediation of emerging vulnerabilities and threats.

7 Business Application Solutions

7.1 Business and Corporate Application Solutions

The department has a complex suite of Business Applications Solutions. There are 155 applications spread out over the eight portfolios.

- **Schools and Early Years** (2 business applications)
- **Development and Support** (50 business applications)
- **Continuous Improvement and Evaluation** (30)
- **Keeping Children Safe** and **Youth Justice** (5 business applications)

- **Business Operations and Support** (64 business applications)
- **Office of Secretary** (2 business applications)

A high proportion of these business application solutions are older than 4 years. Business applications ideally should not be older than 5-7 years, otherwise there is a risk that technology and business requirements have changed too much, and support costs for the business application solutions increase dramatically. The goal should be to retire / re-engineer 15% of the business application solutions per year, which is approximately 23 applications per year. At times the cadence is increased, should operating system or technology stack components approach end-of-life and require replacement.

The department has legacy technology or process delivery still in use that no longer is considered enterprise grade, like Microsoft Access, file sharing via email inboxes, and monolithic spreadsheets in shared drives. These practices are becoming support intensive, create security risks, and are often failing to meet business requirements due to their age, size and the technology used.

Historically the department has developed business application solutions in a disconnected, reactive way. This approach has led to several problems including:

- Lack of project management discipline leading to poorly understood requirements and therefore business application solutions which are poorly aligned to business outcomes.
- Duplication of effort / data across multiple business applications.
- Difficulty in providing whole of department data analysis.
- Inconsistency of data that is stored in multiple business applications eg DECYP site locations in various business applications.
- Poor lifecycle management of the business application solutions including not undertaking regular updates (patches by the software vendors) has led to aging infrastructure (software and hardware), increasing the risk of failure of those business application solutions as well as increasing the risk to data and cyber security.
- Increased support costs for business units and ITS in supporting the multiple business application solutions and technology stacks associated with them.

Strategic Direction

- The department is developing a Roadmap for Business Applications out to 2030. An output from the Roadmap will be a Plan that covers the Business Applications.
- The preference will be for managed Software as a Service (SaaS) applications, rather than the department hosting applications and platforms. Utilising SaaS in line with Whole of Tasmanian Government Cloud strategy.
- Where this is not possible, the department will wherever possible procure off the cloud-based Infrastructure stack (Infrastructure as a Service (IaaS) or Platform as a Service (PaaS).
- The department will preference commercial solutions using industry-standard toolsets and languages with an ‘Adopt and Adapt’ approach rather than build a business application solution as a bespoke solution. Adopt means to adopt the commercial application with minimal changes and adapt our processes to fit in with the selected solution.
- ITS via account meetings with business units will be highlighting on an individual business application solution basis the underlying IT Infrastructure status of the business application,

including those at a higher risk of failure due to the server technology that hosts the application or the underlying software being aged or out of supported.

- Any new business system , significant change to a business system or new data integration must be submitted using the Technology Initiative Request which requires Portfolio Deputy Secretary approval to provide guidance to business and service areas and streamline analysis and procurement, in line with the strategic direction.
- The department utilises the Whole of Tasmanian Government Technology Services Multi-Use List (TSL) panel which includes vendors for a software development and support / services panel of local and interstate companies to enable access to multiple software solutions / technical skill sets to support business application solutions.

Replacement Cycle

This will be developed as part of the Roadmap plan.

7.2 Key Business Application Solutions Managed by IT Services

ITS provide and support a few of the department's base Business Application Solutions.

7.2.1 Content Manager

Content Manager (CM) is currently the main storage system of corporate records across DECYP and is used by all non-school staff for the storage of digital records created by Word, Excel, PowerPoint, eMail. Retention and Disposal schedules and processes are actioned on the CM storage locations on a regular basis to meet Archives Tasmania requirements.

7.2.2 ServiceNow

ServiceNow is the department's core service desk that is used by a number of business units (ITS, PSS, Finance, DSI, Libraries Tas) to manage service requests and incidents from their end users / clients streamlining their support operations, improving productivity, and enhancing customer satisfaction. It enables end users to access self help and knowledge base articles to assist in overcoming minor technical issues.

7.2.3 Identity Management (MyLogin – SailPoint)

The department's Identity Management system (MyLogin) is a contemporary SailPoint based system that uses data from key systems such as Human Resources (Empower) and Student Management System (EduPoint) to enable fine grained automated user provisioning, access, and authorisations based upon the staff or student data in the authoritive business systems. These automated processes overcome manual processes normally in place and provide a far more secure and auditable access for staff and students to business systems and associated data. This platform is constantly receiving feature and quality of life enhancements to support the access and provisioning requirements of the department, as new systems and policies are implemented.

7.2.4 DevOps

Automation of delivery – modern IT business practices like DevOps, and Continuous Integration and Deployment (CI/CD), and automated testing will be leveraged to minimise change risks, lower business application solution downtime, speed up the provision of new services, and create a flexible means to redeploy business application solutions during technology uplift programmes. Automation practices will also provide new ways of ensuring a high continuation of service and a smoother disaster recovery response should issues arise.

8 Artificial Intelligence (AI) Technology

Artificial Intelligence (AI) has generated a substantial amount of media attention over the last twelve months with the release of readily available large language models (LLM) like ChatGPT that can interpret and generate text to a level that closely simulates human conversation.

Whilst AI presents several opportunities for improving technology platforms, it is important to be aware of the risks and limitations of these products. In particular, their predisposition to hallucinate (make up answers to questions) and strong likelihood of introducing unconscious bias that may lead to misrepresentation of or negative outcomes for minority groups that were not adequately represented in the training datasets used by the LLM.

Additionally, commercially available services like ChatGPT are considered high-risk as it's not clear how data entered as prompts into these platforms is consumed and used, nor where it is stored which may ultimately contribute to a cyber breach for the department. IT Services have gained access to Microsoft AI solutions which are hosted securely in the department's cloud network environment and alleviate these risks.

Across Australia, government institutions have been rolling out ChatGPT-like solutions (e.g. South Australia's Education Chat, NswEduChat, QChat in Queensland) that are built in a secure network environment and introduce moderation layers to restrict the data returned from the AI as a way to reduce risk and provide a safe AI experience for the users. Many of these solutions are expected to be either released as open-source and/or made available to other government entities. While the AI toolset might be free, its use within a secure and safe environment controlled by the department will generate usage costs based upon the number and types of prompts used. The South Australia pilot carried out in 2023 costed this usage at $1 per student / staff member per week of use, being several thousands of $s over the school year.

At a policy level there has been significant work in this space with development of several frameworks to guide the use of AI – including the Australian government Department of Industry, Science and Resource AI ethics framework, Australian Government Department of Education Generative Policy and DECYP's own AI policy (centred on schools). Whilst students in classrooms are at higher risk of misinterpreting AI responses, there is an equal requirement to provide guidance to staff in corporate settings around the use of AI.

IT services are currently exploring several AI pilots with different DECYP business areas and industry partners, and expect the outcome of these engagements will guide the technology direction moving forward.

Strategic Direction

- Continue to align to existing federal and state AI policies as they are released or updated
- Observe roll-out of AI solutions by interstate jurisdictions, and use their learnings/technology (where available) to guide technology development.
- Preference multi-use toolsets like Azure OpenAI instead of single-use solutions to reduce cost/risk.
- Leverage pilots within the department to determine local use-cases for AI, and the overarching technology platform strategy.
- Invest in Microsoft AI technology (Copilot and Azure OpenAI) secured within the department's cloud network to manage data and safety risks.
- Ensure any technology component is supported by end user training and advice to ensure users are aware of the risks/limitations associated with their use of AI.

9 Projections of ITS Funding Allocations 2024 – 2029

IT Infrastructure – Capital - BCN 855 Business and service delivery units	2024/25 $	2025/26 $	2026/27 $	2027/28 $	2028/29 $	Total $
1.1 SurfacePro / Laptop devices (Non-school based staff)	134,200	171,600	103,400	1,467,400	3,174,600	5,051,200
1.1 SurfacePro / Laptop devices (Libraries Tas staff)	301,400	15,400	24,200	33,000	66,000	440,000
1.1 Desktop PCs, Portable devices (Libraries Tas public machines)	364,000	74,000	10,000	42,000	62,000	552,000
2.1 Local Area Network (LAN) Switches	182,931	91,267	298,487	537,249	216,368	1,326,302
2.2 Local Area Network (LAN) WAP Installation	17,000	38,143	38,143	38,143	38,143	169,572
2.3 Local Area Network (LAN) WAPs	71,000	100,468	100,468	100,468	100,468	472,872
4.4 Servers	100,000	100,000	0	0	0	0
4.5 Storage (including backup and recovery)	0	100,000	200,000	200,000	200,000	700,000
5.1 Telephone Services	20,000	20,000	20,000	20,000	20,000	100,000
5.2 Video Conferencing - Surface Hubs	871,000	91,000	13,000	338,000	338,000	1,651,000
Total	**2,061,531**	**801,878**	**807,698**	**2,776,260**	**4,215,579**	**10,662,946**

IT Infrastructure – Recurrent - BCN 855 Business and service delivery units	2024/25 $	2025/26 $	2026/27 $	2027/28 $	2028/29 $	Total $
1.1 Desktop PCs and Portable devices	8,000	8,000	8,000	8,000	8,000	40,000
1.2 Software - SOE software	914,953	914,953	914,953	1,010,000	1,010,000	4,764,859
1.3 Printers and Multi-Function Devices	0	0	0	37,500	0	37,500
1.4 IT Support Costs	110,000	115,000	120,000	125,000	130,000	600,000
2.1 Local Area Network (LAN) Switches	10,465	15,765	34,600	66,245	79,310	206,385
2.2 Local Area Network (LAN) Cabling	30,000	30,000	30,000	30,000	30,000	150,000
2.3 Local Area Network (LAN) WAPs	62,000	63,000	64,500	66,000	68,000	323,500
2.4 Network Monitoring and Management	90,000	145,000	150,000	155,000	160,000	700,000
3.1 Wide Area Network (WAN)	1,800,000	1,850,000	1,900,000	2,000,000	2,100,000	9,650,000
3.2 Remote Access	10,000	11,000	12,000	13,000	14,000	60,000
4.1 Cloud Compute (IaaS or PaaS)	3,300,000	3,400,000	3,500,000	3,600,000	3,700,000	17,500,000
4.2 Servers - physical and logical	250,000	260,000	270,000	280,000	290,000	1,350,000
4.3 Server Operating System (OS)	0	0	0	0	0	0
4.4. Backup and Recovery	209,000	209,000	209,000	209,000	209,000	1,045,000
4.5. Data Platforms	340,000	350,000	360,000	370,000	380,000	1,800,000
4.6. Facility Management and Hosting	200,000	200,000	200,000	200,000	200,000	1,000,000
5.1 Telephone Services	250,000	260,000	270,000	280,000	290,000	1,350,000
6. Cyber Security	450,000	450,000	450,000	450,000	450,000	2,250,000
7. Business and Corporate Applications Support	850,000	890,000	930,000	970,000	1,010,000	4,650,000
7.2.1 Content Manager	280,000	300,000	320,000	340,000	360,000	1,600,000
7.2.2 ServiceNow	450,000	450,000	450,000	480,000	480,000	2,310,000
7.2.3 MyLogin	600,000	620,000	640,000	660,000	680,000	3,200,000
Total:	**10,214,418**	**10,541,718**	**10,833,053**	**11,349,745**	**11,648,310**	**54,587,244**

Total - Capital + Recurrent	**12,275,949**	**11,343,596**	**11,640,751**	**14,126,005**	**15,863,889**	**65,250,190**

IT Infrastructure – Capital - BCN 823 Schools	2024/25 $	2025/26 $	2026/27 $	2027/28 $	2028/29 $	Total $
1.1 Device refresh Teacher's award	60,000	60,000	60,000	60,000	12,000,000	12,240,000
1.1 Device refresh Support staff	2,370,000	450,000	900,000	100,000	100,000	3,920,000
1.1 Device refresh Admin staff	50,000	50,000	1,496,000	50,000	50,000	1,696,000
1.1 Device refresh Yr 11 12 Extension	0	1,040,000	0	0	0	1,040,000
1.1 Device refresh Digital Inclusion Loans	0	0	1,235,000	0	0	1,235,000
2.1 Local Area Network (LAN) Switches	2,093,000	2,095,000	1,882,000	1,611,000	1,897,000	9,578,000
2.2 Local Area Network (LAN) WAP Installation	410,000	410,000	347,000	310,400	347,000	1,824,400
2.3 Local Area Network (LAN) WAPs	1,768,000	1,390,000	1,768,000	1,390,000	1,768,000	8,084,000
4.2 Servers (in Schools)	700000	0	0	0	0	700,000
4.6. Facility Management and Hosting	486000	0	0	0	0	486,000
Total:	**7,937,000**	**5,495,000**	**7,688,000**	**3,521,400**	**16,162,000**	**40,803,400**

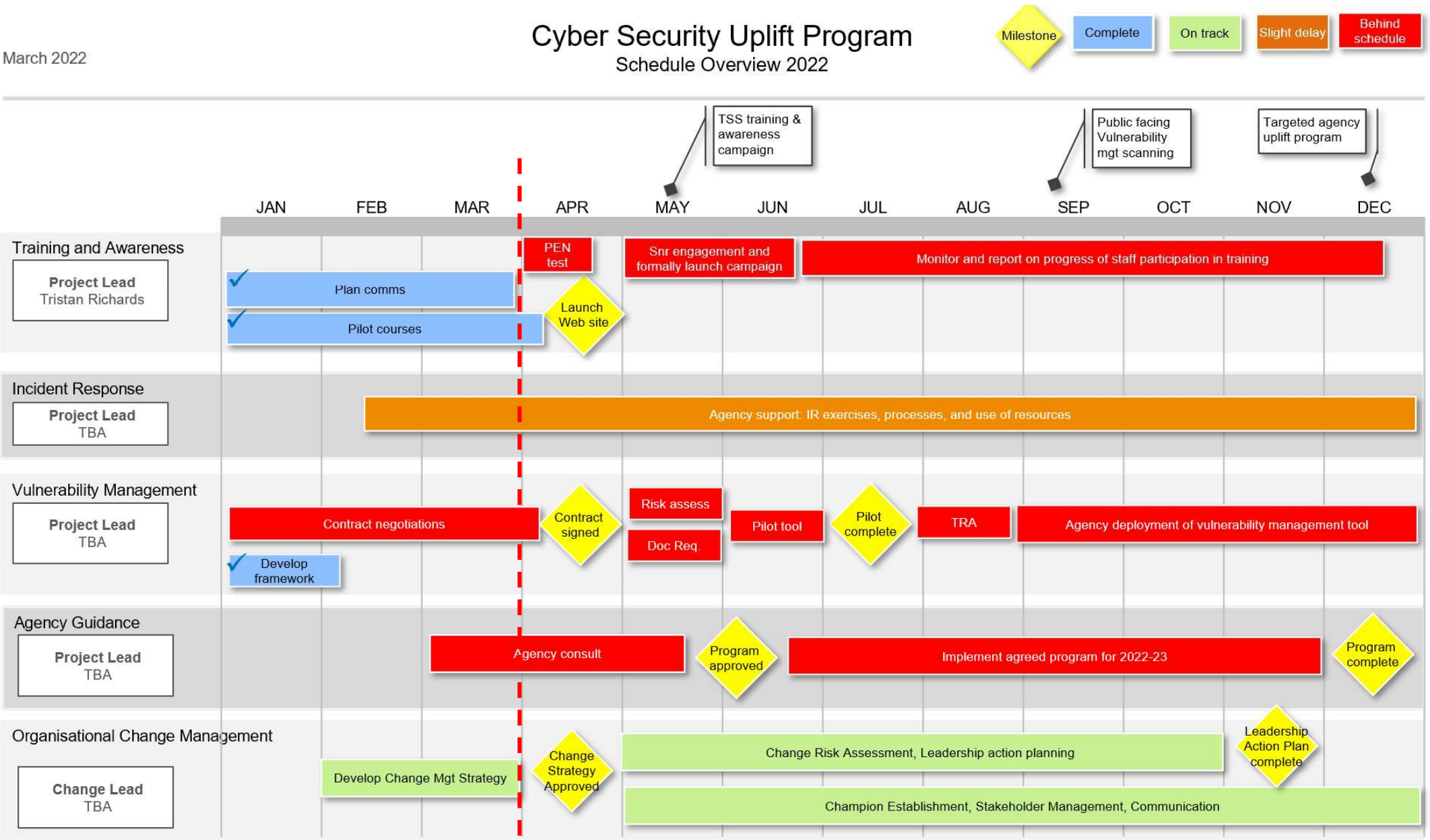
IT Infrastructure – Recurrent - BCN 823 Schools	2024/25 $	2025/26 $	2026/27 $	2027/28 $	2028/29 $	Total $
1.1 Desktop computers, laptops and tablets	36,000	36,000	36,000	36,000	36,000	180,000
1.2 Software - SOE software	450,000	450,000	450,000	500,000	500,000	2,350,000
1.2 Software - CMP software	946,000	946,000	946,000	946,000	946,000	4,730,000
1.3 Printers and Multi-Function Devices	0	0	0	37,500	0	37,500
1.4 IT Support Costs	1,500	1,500	1,500	1,500	1,500	7,500
2.1 Local Area Network (LAN) Switches	130,500	253,400	366,000	467,000	572,500	1,789,400
2.2 Local Area Network (LAN) cabling	30,000	30,000	30,000	30,000	30,000	150,000
2.3 Wifi	636,000	636,000	636,000	636,000	636,000	3,180,000
2.4 Network Monitoring and Management	160,000	1,160,000	1,160,000	1,160,000	1,160,000	4,800,000
3.1 Wide Area Network (WAN)	4,200,000	4,200,000	4,200,000	4,200,000	4,200,000	21,000,000
3.2 Remote Access	350,000	350,000	350,000	350,000	350,000	1,750,000
4.1 Cloud Platforms	0	0	0	0	0	0
4.4 Storage (including backup and recovery)	60,000	65,000	70,000	75,000	80,000	350,000
5.2 Video Conferencing - Microsoft Teams	0	0	0	0	0	0
7.2.2 ServiceNow	450,000	450,000	450,000	480,000	480,000	2,310,000
Total:	**7,414,000**	**8,541,900**	**8,659,500**	**8,883,000**	**8,956,000**	**42,454,400**

Attachment H

March 2022

Cyber Security Uplift Program

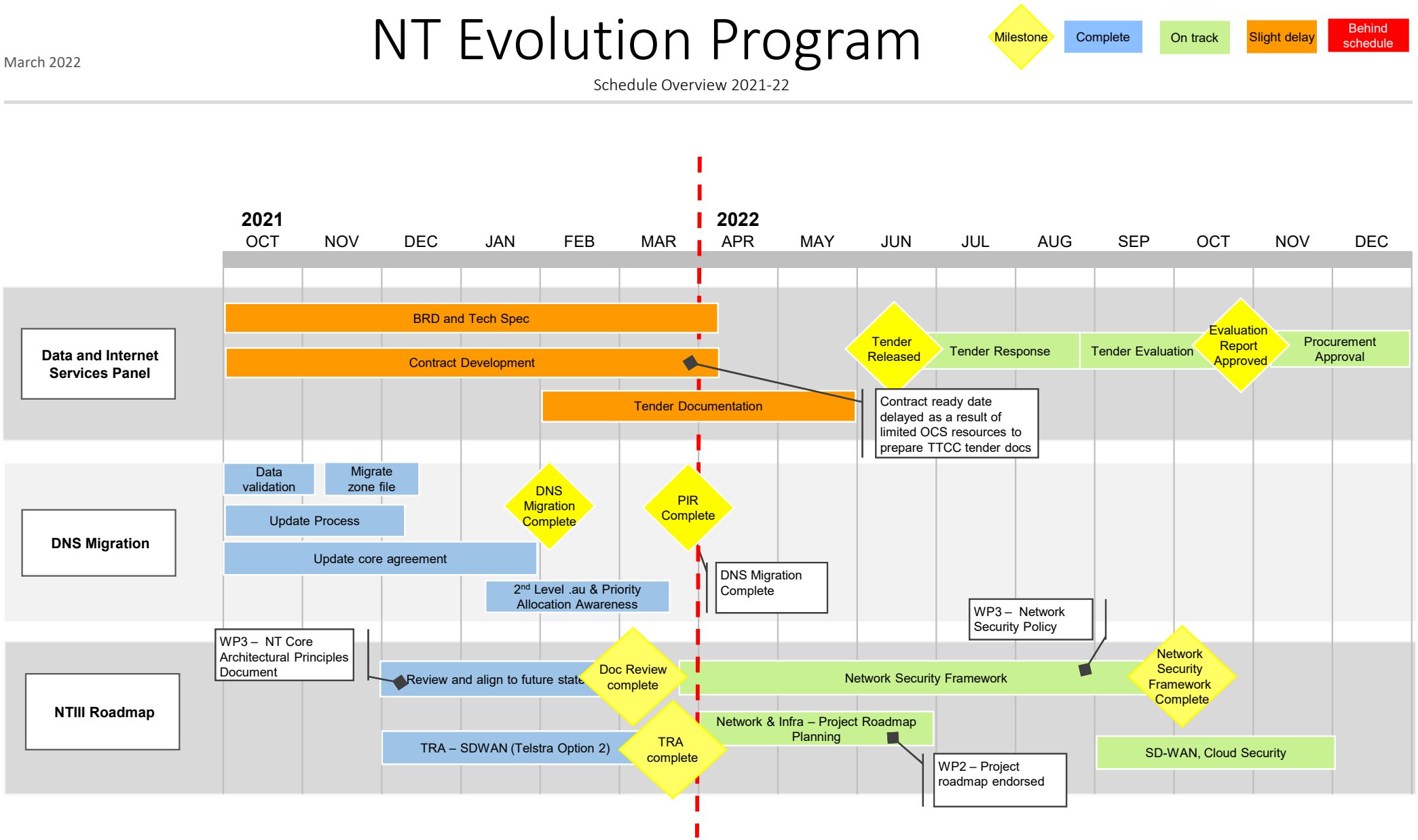
Schedule Overview 2022



March 2022

NT Evolution Program

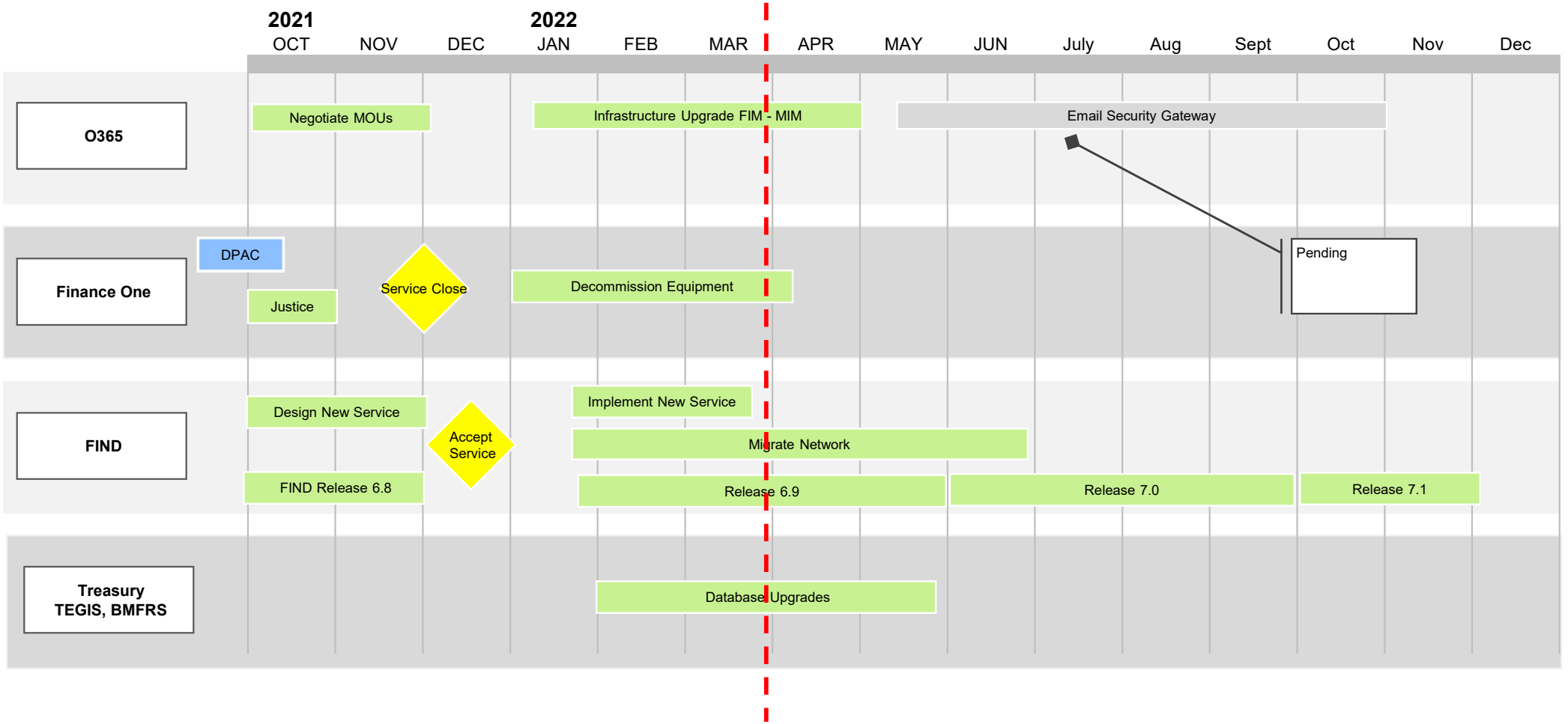
Schedule Overview 2021-22



Applications

October 2021
Schedule Overview 2021-22

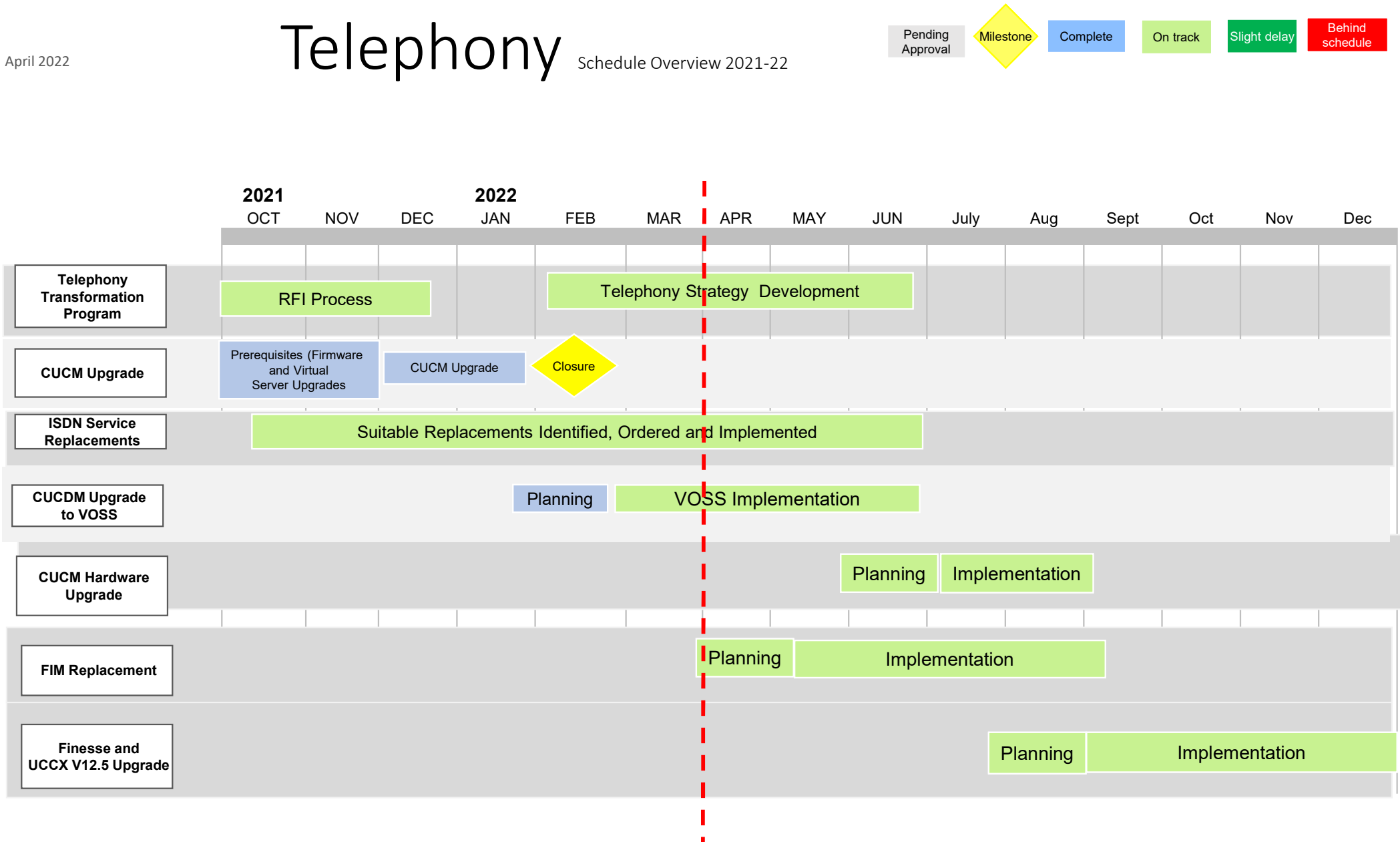
Pending Approval | Milestone | Complete | On track | Slight delay | Behind schedule



April 2022

Telephony

Schedule Overview 2021-22

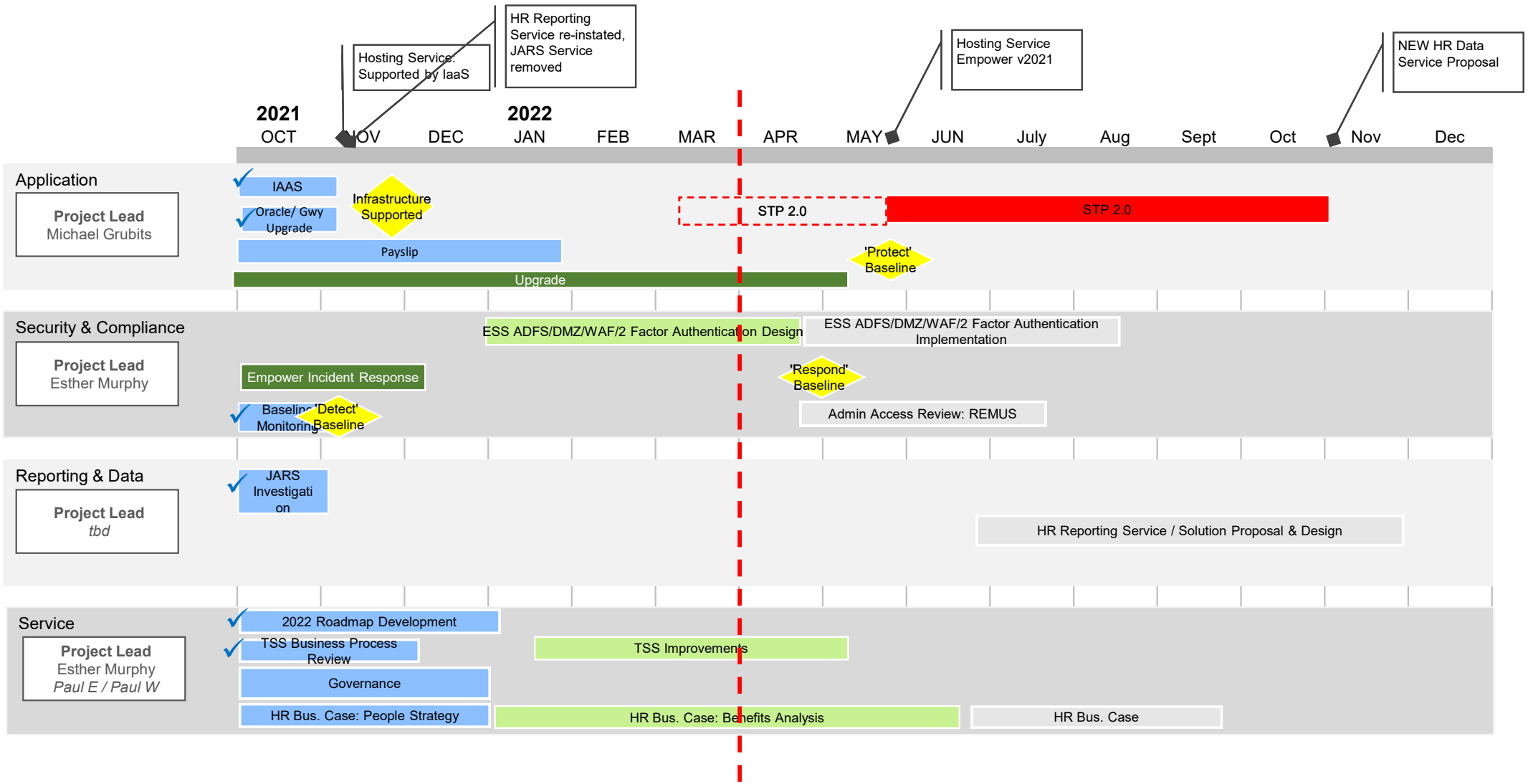


October 2021

HR Applications

Schedule Overview 2021-22

Pending Approval | Milestone | Complete | On track | Slight delay | Behind schedule



Strategic Roadmap – Networks and Infrastructure

PURPOSE	SERVICE OR FUNCTION:
To provide Tasmanian Government agencies with access to contemporary, fit-for-purpose ICT networks and infrastructure to support their business needs.	**Networks and Infrastructure**

CURRENT STATE 2022

List 5 to 10 dot points describing the current state.

- Contracts in place across majority of aspects of networks and infrastructure (with exception of public cloud). Extensions generally available to 2027/29.
    - Single vendor for Core (Telstra, contract extended to May 2027)
    - Panel arrangements for other services
- Contract model is mature but based on ProcureIT rather than TTCC
- Network and security posture based on hub/spoke architecture with access generally based on IP rather than identity. This is no longer contemporary and requires refresh.
- No whole of Government network security policy or guidance. Current NT contracts based on Telstra contracted as primary security responsibility.
- Visibility/reporting/self-serve functionality is not contemporary or fit for purpose
- Telstra (key NT Supplier) not meeting agency expectations for service provisioning and continuous improvement
- Inadequate DSS resources to manage suppliers, services and agency relationships
- Pricing not regularly reviewed, potentially resulting in reduced value for money
- TIP lacks agency support – desire to move to MS
- CF product is approaching end of life
- No whole of Government approach to public cloud procurement or deployment (Cloud first policy in place, but no contracts or guidelines to support).

PRIORITIES

List up to five priorities for your work plan

1. **Establish DSS Networks and Infrastructure team** – resources, relationships and processes – as a respected and valued agency and vendor partner
2. Continue to **progress the NT Evolution program**
3. **Review public cloud services in Tasmanian Government** – how these are procured and implemented, potential gains to be made through a consistent WoG approach
4. Participate in and contribute to the **development of the whole of Government Technology Roadmap for Networks**

ASSUMPTIONS

List any underlying assumptions

1. Development of Networks and Infrastructure services is in accordance with relevant whole of Government and DPAC policies and frameworks (which exist or can be developed where required)
2. Decision making is in line with DSS delegations and done in consultation with Agencies
3. Appropriate Governance mechanisms are in place and operating effectively

TARGET STATE 2025

List 5 to 10 dot points describing the desired target state.

- Networks and Infrastructure team on board and established (BAU processes, practices, etc)
- Regular open dialogue with agencies (formal and informal, strategic, tactical and operational)
- Supplier relationships uplifted and effective at strategic, tactical and operational levels
    - Agencies have seen significant improvement to Telstra engagement and performance
- NT Evolution program complete:
    - NT3 capacity uplift complete
    - Agencies able to implement distributed architecture at scale
    - Contemporary services offerings in place for Email Filtering and Web Content Filtering
    - NT3 reporting and service management functionality contemporary and fit for purpose
    - Revised core cost model in place and accepted by agencies
- Risk management framework in place for Networking Tasmania services. Clear guidance exists on required network security controls and new services can be implemented quickly and securely
- Clear WoG guidance on procurement and utilisation of public cloud services. Expect utilisation of these services to be significantly increased
- Clear strategy in place for the next iteration of Network & Infrastructure services (“beyond NT3”). Next steps defined and agreed, necessary procurement processes underway.

Data and Digital Committee

Terms of Reference

Purpose	A standing subcommittee of the Secretaries Board, the Data and Digital Committee is to: • oversee whole of government digital initiatives (including the TSSR 'digital enhancement' recommendations) • monitor progress and the delivery of significant government digital priorities (including *Our Digital Future*) • lead engagement and collaboration across government agencies to promote a user-focused, and 'one government' approach to the design and delivery of digital services • facilitate the establishment of effective data governance and data sharing capabilities across government.
Chair and Members	The Committee will be chaired by the Deputy Secretary, Government Services, Department of Premier and Cabinet (DPAC). The Committee membership comprises the Tasmanian Government Chief Information Officer, and Data and/or Digital leads from the departments of/for: • Premier and Cabinet • Treasury • Education, Children and Young People • Health • Justice • Police, Fire and Emergency Management • Natural Resources and Environment • State Growth The Committee may also co-opt additional specialist representatives aligned with Government priorities, at the invitation of the Chair.
Responsibilities	The responsibilities of the Data and Digital Committee are to: • Submit an annual work program to the Secretaries Board for approval; • Oversee the Board-approved work program, only including additional items with the approval of the Secretaries Board (or its Chair); • Develop strategies to address TSS-wide issues and make recommendations to the Secretaries Board; • Provide advice to the Secretaries Board and relevant committees on emerging data and digital issues; • Work collaboratively with the other subcommittees to ensure consistent advice and approach.

	The Data and Digital Committee's role may vary with respect to individual initiatives/ projects, or in response to specific direction from the Secretaries Board, to include: • Sponsorship/ advocacy • Advice • Leadership • Collaboration
Reporting	The Data and Digital Committee will: • submit an annual work program to the Secretaries Board for approval; • provide monthly reports to the Secretaries Board; and • provide verbal updates to the Secretaries Board on request. *(Verbal updates may be provided by a subject matter expert who is not a member of the Data and Digital Subcommittee, by nomination of the Data and Digital Subcommittee Chair, and by agreement of the Chair of the Secretaries Board)* The Secretaries Board notes that due to key person dependencies, the occurrence of cyber incidents may impact priorities and delivery dates of the DDC workplan.
Meetings	Meetings will be scheduled monthly, or as advised by the Chair. The Secretariat will be provided by the Digital Strategy and Services (DSS) division, DPAC. The Secretariat will prepare the agenda for approval by the Chair. Committee members may request to have additional items added to the meeting agenda to the Chair via the Secretariat.
Conflict of Interest	Members must disclose, and take reasonable steps to avoid, any conflict of interest connected with their role on the Committee.
Attendance and Absences	The Chair may nominate another Committee member to preside at any meeting where the chairperson is unable to be present or has a conflict of interest in the matter being discussed. Unless formal acting arrangements are in place, proxies must be approved by the Chair prior to attending a meeting to represent their agency. Committee members can seek approval from the Chair to bring a colleague or colleagues with relevant subject matter expertise to participate in discussion of a specific agenda item.
Working/ Reference Groups	The Data and Digital Committee may create and oversee temporary/ ongoing working or reference groups to support its work program.
Review	The Committee may propose changes to its Terms of Reference for approval by the Secretaries Board, at any time.

Our Digital Future Progress 2024-25

Priority 1 - Our Digital Community

All Tasmanians should have an equal opportunity to interact with digital services and information in ways that are easy to use, convenient and readily available.

Ref	Action	Lead	Status	Achievements
1.1	Deliver the Digital Ready for Daily Life program for digitally disadvantaged groups, including low-income households, older Tasmanians, and people not in paid employment	DSG	Completed	• The *Digital Ready for Daily Life* program led by the Department of State Growth provides targeted digital assistance to vulnerable community members. This program is working with the Department for Education, Children and Young People's 26TEN initiative, to embed digital trainers in their *Local Literacy for Work and Life* program locations. Digital assistance and capacity building are being provided in the original four 26TEN communities (Glenorchy, Clarence Plains, Launceston Northern Suburbs, and the Huon Valley) in 2024-25. The Government committed an additional $700 000 over 4 years to the Digital Ready for Daily Life Program in 2021-22, which aims to improve the digital skills of Tasmanians, particularly the more vulnerable in our community.
1.2	Strengthen opportunities for lifelong digital skills learning	Libraries Tasmania	Completed, Ongoing.	• Libraries Tasmania provides a range of services designed to build the digital ability within the Tasmanian community. • At 46 public libraries across the state, Libraries Tasmania supports digital inclusion for Tasmanians by providing free high-speed Wi-Fi and access to more than 500 devices. • Hundreds of trained staff and volunteers provide digital help for all ages through one-to-one and group sessions. • The digital help programs explore using smartphones, email and the internet. One-to-one help includes a range of assistance such as navigating digital government services and troubleshooting digital problems. These programs allow the community to receive personalised, face-to-face help in their local area. • Through the 26Ten Coalition and the Adult Literacy Service, Libraries Tasmania also offers free learning programs to develop literacy and numeracy which are foundational to developing digital skills.
1.3	Provide more options and opportunities for public access to 'anytime, anywhere' government services	DSG, DPAC, DOE	Completed, Ongoing.	• The Tasmanian Government successfully leveraged the rollout of the NBN and the Commonwealth Regional Connectivity Program and the Mobile Blackspot Program to provide improved access to services in regional communities, with a particular focus on communities with low socioeconomic status, linking digital access with state educational programs. • To ensure Tasmanians can easily access government services and information, Service Tasmania has focused on a significant redevelopment of their online presence with a an updated www.service.tas.gov.au and the implementation of the myServcieTAS portal.

1.4	Improve telecommunications infrastructure, particularly in rural and regional Tasmania	DSG	Completed	• The Tasmanian Government invested $1.6 million in Tasmanian digital infrastructure development through its partnerships with the Australian Government under both the Mobile Black Spot and Regional Connectivity Programs. • DECYP was successful in obtaining funding through the Regional Connectivity Program, a joint venture with Telstra.
1.5	Increase 'smart city' technology to support urban communities and new technology businesses	DSG	Completed.	• State Growth spatial services group supported the infrastructure policy team and LGA/Councils with the delivery of the Smart Cities initiative. • Program established in Launceston.
1.6	Support transformative digital projects that improve the delivery of frontline services to Tasmanians	DPAC	In delivery, Ongoing.	• Service Tasmania Customer Experience Program • Completed redevelopment of the Service Tasmania website to make it easier for Tasmanians to find the government services they need, • Completed myServiceTAS digital portal to provide Tasmanians with a secure and easy-to-use access point for Government services. • Additional projects – Justice Connect, Plan Build, Health Digital Transformation Strategy.

Priority 2 - Our Digital Economy

Tasmania's economy will be bolstered by the competitive advantage, productivity growth and prosperity enabled by knowledge-driven digital transformation.

Ref	Action	Lead	Status	Achievements
2.1	Empower local businesses through the Digital Ready for Business program	DSG	In delivery, substantial progress.	• Running the Digital Ready for Business program to improve the digital capability, literacy and confidence of small businesses by empowering them to make better digital economy decisions. $1 million has been provided to the program through to 2025.
2.2	Work with industry, business and education partners to develop and promote digital education, career pathways and workforce capability	DSG (Skills), DPAC	In delivery, Ongoing.	• The Government worked closely with industry and education stakeholders in sponsoring the Tasmanian ICT Workforce Development Program, which included an industry capability survey. • TASTAFE cyber security pathways • The Tasmanian Government Chief Information Officer is a member of TASIC for spatial industry • Skills TAS industry accord • Tasmanian Government Workforce Development program
2.3	Accelerate technology startups and entrepreneurial pathways through targeted programs supported by the Office of the Coordinator-General	OCG	Completed, Ongoing.	• Established Enterprize Innovation Hubs to foster entrepreneurship and support start-ups across the state. Hubs were focused on providing the resources and support required to inspire and accelerate students, innovators and entrepreneurs.
2.4	Build the export capabilities of technology businesses through the Tasmanian Trade Strategy 2019–2025	DSG	In delivery, substantial progress.	• Advanced technologies program • USA Trade Mission
2.5	Uplift the global branding of Tasmania's information technology industry	DSG	In delivery	• industry support through events such as TASICT conference and awards • USA Trade Mission
2.6	Work with industry providers to enhance the adequacy and reliability of Tasmania's digital communications infrastructure	DSG, DPAC	In delivery, needs attention to progress in a meaningful way.	• DSG have been working with the Telecommunications sector. • Subsea cable business case, project failed to obtain federal funding. • Tasmanian Disaster Risk Assessment exercise undertaken to provide insight and understanding around large scale disruption to digital communications infrastructure.

Priority 3 - Our Digital Government

All Tasmanians should have an equal opportunity to interact with digital services and information in ways that are easy to use, convenient and readily available.

Ref	Action	Lead	Status	Achievements
3.1	Develop new frameworks for information management and data analytics	OSA, DSS	In delivery Substantial progress	The Office of the State Archivist (OSA) published new Tasmanian Government Information Management Framework Active initiative under the Digital and Data Sub Committee of the Secretaries Board work program, being progressed by Data and IM Working Group to develop a new / revised framework that addresses critical aspects of information and data management – leadership, strategy, governance and information asset management and to facilitate the development of a roadmap to establish the foundational capability for information management, data sharing and analytics across government (to support further progress and a business case toward Recommendation #19 of the Tasmanian State Service Review). Recommendation #50 of the PESRAC Report - Data Sharing Business Case which was completed in 2021, incorporated into TSSR as Recommendation #19 - that the government develop and fund a stronger whole-of-government capability for sharing, linking and analysing data and assign a functional leader to deliver services to, or build capability across, all agencies.
3.2	Develop a whole-of-government technology roadmap	DSS	In delivery	The Critical systems and ICT infrastructure audit recommended that the Government develop a vision and strategy for ICT investments, and form part of audit response. Active initiative under the Digital and Data Sub Committee of the Secretaries Board work program - whole-of-government digital capability and technology roadmap, to develop a digitalisation or digital capability roadmap for government that is aligned to the priorities set out for government in Our Digital Future and will support the vision for digitalisation reform in the TSSR.
3.3	Adopt a cloud-first policy approach across government agencies	DSS	Complete	Transition to cloud is well progressed across most agencies. Represents significant transformation in ICT services. Tasmanian Government Cloud Policy has been in place for more than three years.

Ref	Action	Lead	Status	Achievements
3.4	Implement a cybersecurity program that prioritises critical asset protection across government	DSS	Complete	Four-year program established and funded in FY2020/21 to address several critical risk areas – Funded over 4 years. New cyber security and resilience strategy 2023-2027 is under development. Cyber-hubs initiative funded in 2023-24 Budget.
3.5	Develop digital culture and capability across government agencies	All	In delivery, but not in a formal way.	Many agencies are progressing their digital maturity, however, there has not been a transition towards the now general accepted digital culture practices we would see in other jurisdictions or in the commercial sector. Service Tasmania has commenced implementation of its Business Strategy which requires the development of the same culture, Service Tasmania is also focusing on integrated customer journey development – Life Events.
3.6	Streamline government processes for the procurement of technology services	Treasury, OCS	Complete	Government Information Technology Contract and IT Professional Services Panel overhaul completed implemented as Tasmanian Technology Contract Conditions and Technology Services List respectively.
3.7	Reduce government red tape through the adoption of digital solutions	OCG	In delivery Substantial Progress	The Red Tape Reduction Coordinator consults extensively with business and industry to nominate red-tape issues and has a portal for stakeholders to lodge red tape issues for investigation. The following initiatives have progressed to address red tape issues using digital solutions. - Fisheries Digital Transition Project - Transitioning commercial fisheries to digital processes, including the FishPort web portal and FishReport mobile application. - PlanBuild Tasmania Portal - Streamlining the process for lodging and assessing planning, building, and other applications to local councils. - myServiceTas Digital Services Portal - Developing a secure, easy-to-use access point for government services, including driver license renewals and vehicle registration.

Ref	Action	Lead	Status	Achievements
				- Online Firearms Management System - Implementing an online portal for firearms license holders and dealers to improve transactions with Firearms Services.
3.8	Develop an agile, iterative and risk-managed approach to the management and delivery of digital projects and services	All	In delivery, but not in a formal way.	This is a default position for most agencies – principally that they take a risk-managed approach to the management and delivery of digital projects and services. DSS facilitates an active and successful community of practice in design thinking.

NRE Tas

Information Asset Register - List Column (field) Definitions

Column Name	Column Description	Section	Column Supporting Comments	Column Restrictions
Asset Code	Unique ID of Asset	Summary	Format - IA XXX	DDS staff only
Asset Name	The name or title of the information asset	Summary	i.e. Water Information Management System	All
Asset Short Name	Short name or acronym of the information asset	Summary	i.e. WIMS	All
Asset Description	Description of the contents and / or an outline of the components of the asset	Summary	Provide a detailed description of the asset. Can include what it does, who uses it, upgrade plans, any relevant information	All
Asset Category	What category of asset	Summary	Application, infrastructure or platform	All
Location	Where is the asset located/hosted	Summary	Options: On-Prem, SaaS, NRE DC, NRE Cloud, Azure, Aws	DDS Staff Only
Type of Application	The functional type of asset	Summary	i.e. booking system, emergency management, human resources	All
Supported By	Party responsible for supporting asset	Summary	i.e. Vendor, NRE ICT, Contractor	All
Vendor	Vendor of the asset	Summary	Specify vendor of the asset if selected in 'supported by' field	All
Status	Current status of the asset	Summary	Active, development or Inactive (do not use NEW)	All
General Comments	Generalised information if required	Summary	Add any other information here that doesn't fit into asset description field	All
Department	Owner of the asset Note: owner has been split into a hierarchy of Department > Division > Strategic Business Unit > Branch to simplify grouping and filtering.	Business Owner	Who owns the asset. May be another Tas Gov jurisdiction. If unsure ask DDS. If not NRE, still fill out below fields, stating who within NRE is responsible for the asset	All
Division	see above	Business Owner	i.e. Strategy and Business Services	All
Strategic Business Unit	see above	Business Owner	i.e. Business Services	All
Branch	see above	Business Owner	i.e. Digital and Data Services	All
Risk/System Owner	Risk/system owner of the asset	Business Owner	Nominated individual within NRE who is responsible for the system and associated risk	All
Administrator	Administrator of the asset	Business Owner	Can be risk/system owner, or another individual. Whoever is making changes to the asset within NRE	All
Administrator - External	External administrator of the asset	Business Owner	Individuals name, could be a vendor or contractor	All
Business Contact - External	External contact for the asset	Business Owner	Individuals name, could be a vendor or contractor	All
Internal Cohorts	Relevant internal cohorts the asset encompasses	Business Owner	i.e. whole of government, NRE exec, multi-agency	All
External Cohorts	Relevant external cohorts the asset encompasses	Business Owner	i.e. Industry, Community, Visitors, Other	All
Revenue	Does this asset contribute revenue for the agency or customers? Or involve significant $ transactions.	Asset Score	0 = No revenue 1 = up to $500k revenue or less 2 = up to $1M revenue or less 3 = up to $5M or less 4 = $5M revenue and above	All
Reputation	Impact to reputation of the agency, WoG, or Tasmania. Does loss of availability of information or systems affect any party's reputation? Issues to consider include potential for adverse publicity, either locally or wider and the potential for damage occurring to either the service provider's or client's ongoing reputation due to information being unavailable.	Asset Score	0 = no reputational impact 1 = Attention from a stakeholder with no broader exposure 2 = Localized short duration media interest/negative exposure, Minister concerned	All

			3 = Multiple media channels reports/negative exposure, Minister Questioned 4 = Widespread public concern or dissatisfaction, Loss of confidence and trust in the government of the day. Persistent parliamentary scrutiny	
Service	Impact on ability to deliver services by NRE Tas or Service delivery by other Agencies we support to all stakeholders including the public	Asset Score	0 = No impact 1 = one or more services reduced or impeded, no stakeholder impact, other services unaffected, workarounds available 2 = one or more services is reduced or impeded, minor stakeholder impact, other services are affected, no workarounds 3 = one or more services unavailable, moderate impact to stakeholders, NRE and stakeholders can still provide key services, no workarounds 4 = multiple services unavailable, significant impact to stakeholders, NRE or stakeholders cannot provide key services, no workarounds, shit is on fire	All
Data	Does data held or transferred by the asset have cultural, industrial, scientific, financial or personal value or significance	Asset Score	0 = Data has minimal value and if lost or exposed, no attempts would be made to recover it 1 = Data has a some value and/or exposure loss could be recovered from with minimal effort and cost 2 = Data has considerable value and/or exposure or loss would require moderate effort/cost recover from 3 = Data has substantial value and/or exposure or loss would require substantial effort/cost to recover from 4 = Data exposure or loss would be catastrophic and damage from its loss is not possible to reverse	All
Emergency	Does this asset contribute an emergency response function or service	Asset Score	0 = no function or service 1 = non-critical function or service 2 = critical function or service	All
Asset Score	Total score of the asset	Asset Score	sum of reputation + revenue + data + service + emergency read-only, cannot be manually changed	Read Only
Asset Ranking	Asset ranking among other assets, based on asset score	Asset Score	read-only, cannot be manually changed	Read Only
OS	Operating System	Infrastructure Services	Operating system of the endpoints or supporting infrastructure	INF Staff Only
External	List external-facing endpoints that serve the application/system/asset	Infrastructure Services	i.e. thelist.tas.gov.au	INF Staff Only
Internal	List external-facing endpoints that serve the application/system/asset	Infrastructure Services	i.e. security.thelist.tas.gov.au	INF Staff Only
Production Servers	Production servers hosting asset	Infrastructure Services	names of production servers	INF Staff Only
Dev/test servers	development or test servers hosting asset	Infrastructure Services	names of dev or test servers	INF Staff Only
Infrastructure Comments	Provide comments that may be relevant, i.e., HA, load-balancing, dependencies. links to further information, etc	Infrastructure Services	anything that doesn't fit into pre set fields	INF Staff Only
Cloud Adoption	Cloud adoption required/planned for asset hosting	Infrastructure Services	N/A if no options fit, i.e. already SaaS	INF Staff Only
Primary Support Contact	Main support contact for internally developed assets	System Services	Intended only for system services staff	SS Staff Only
Alternative Support Contact	alternative support contact for internally developed assets	System Services	Intended only for system services staff	SS Staff Only
Risk Comments		System Services		SS Staff Only
Public	Is the asset publicly accessible	System Services	yes or no	SS Staff Only
Issues Register	Internal JIRA issues register for asset	System Services	link to JIRA project	SS Staff Only
Technology Used	List of technologies used in asset	System Services	i.e. JAVA, Springboot, .Net	SS Staff Only

Source Code Repo	Source code GITLAB repository	System Services	link to repo	SS Staff Only
MFA	Status of MFA for the asset	Protective Security	if assets utilising SSO answer is yes	PS Staff Only
Risk Assessment	Does the asset have a cyber risk assessment completed	Protective Security	yes or no	PS Staff Only
Risk Assessment Link	Link to completed cyber risk assessment	Protective Security	can put comments in extra box if required	PS Staff Only
Risk Assessment Date	Date of last risk assessment	Protective Security	Date most recent risk assessment or review performed	PS Staff Only
Does the system integrate with MyDas	Does the system integrate with MyDas	CIS	yes or no	CIS Staff Only
Does the system have the required archival component	Does the system have the required archival component	CIS	yes or no	CIS Staff Only
Do the business outcomes need to be in MyDas	Do the business outcomes need to be in MyDas	CIS	yes or no	CIS Staff Only
CIS Comments	General comments	CIS	Anything relevant that doesn't fit into previous fields	CIS Staff Only
PII (Personal Information)	Does the asset contain/store PII	Personably Identifiable Information	Yes or no	All
PII Persons Name	Does the asset store/contain a users full name	Personably Identifiable Information	tick if yes	All
PII Address	Does the asset store/contain a users address	Personably Identifiable Information	tick if yes	All
PII Email	Does the asset store/contain a users email address	Personably Identifiable Information	tick if yes	All
PII Mobile	Does the asset store/contain a users mobile number	Personably Identifiable Information	tick if yes	All
PII Persons Organisation	Does the asset store/contain a users organisation	Personably Identifiable Information	tick if yes	All
PII Birth Date	Does the asset store/contain a users birth date	Personably Identifiable Information	tick if yes	All
PII Credit Card	Does the asset store/contain a users credit card information	Personably Identifiable Information	tick if yes	All
PII ID Sighted	Does the asset store/contain that a users ID has been sighted (no info stored)	Personably Identifiable Information	tick if yes	All
PII ID Stored	Does the asset store/contain a users ID information (picture or data)	Personably Identifiable Information	tick if yes	All
Gender	Have the gender selection fields been updated to reflect new policy	Personably Identifiable Information	Internally developed apps only	SS Staff Only
Crown Jewel	Is asset a crown jewel	Other	used by protective security staff only	PS Staff Only