Tasmanian
Audit Office

Report of the Auditor-General

No. 4 of 2020-21

Information and communications technology strategy, critical systems and investment

27 October 2020

Strive • Lead • Excel | *To Make a Difference*

The Role of the Auditor-General

The Auditor-General's roles and responsibilities, and therefore of the Tasmanian Audit Office, are set out in the *Audit Act 2008* (Audit Act). The Auditor-General's role as Parliament's auditor is unique.

Our primary responsibility is to conduct financial or 'attest' audits of the annual financial reports of State entities. State entities are defined in the Interpretation section of the Audit Act. We also audit those elements of the Treasurer's Annual Financial Report reporting on financial transactions in the Public Account, the General Government Sector and the Total State Sector.

Audits of financial reports are designed to add credibility to assertions made by accountable authorities in preparing their financial reports, enhancing their value to end users. Following financial audits, we report findings and outcomes to Parliament.

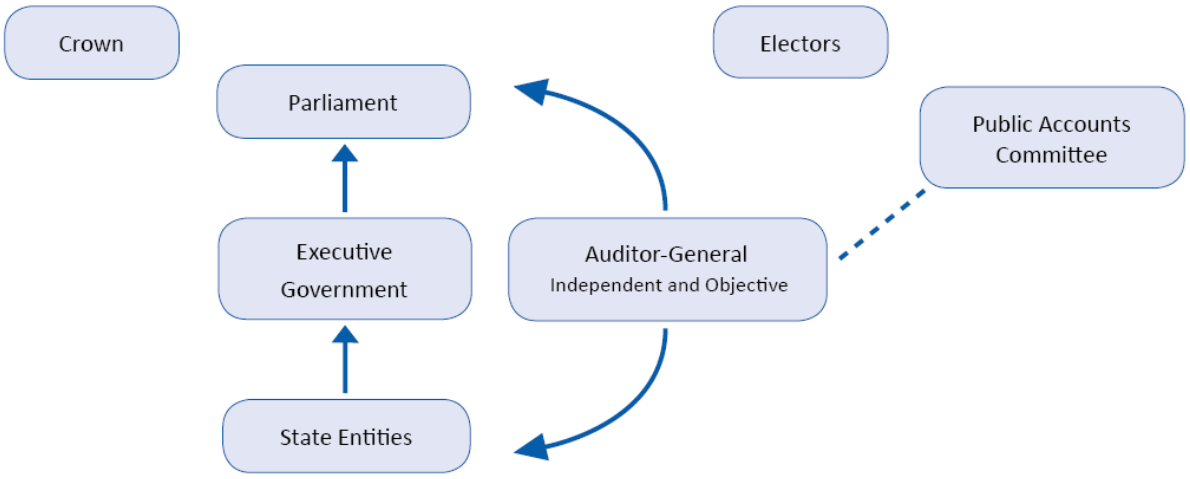
We also conduct performance audits and compliance audits. Performance audits examine whether a State entity is carrying out its activities effectively and doing so economically and efficiently. Audits may cover all or part of a State entity's operations, or consider particular issues across a number of State entities.

Compliance audits are aimed at ensuring compliance by State entities with directives, regulations and appropriate internal control procedures. Audits focus on selected systems (including information technology systems), account balances or projects.

We can also carry out investigations but only relating to public money or to public property. In addition, the Auditor-General is now responsible for state service employer investigations.

Where relevant, the Treasurer, a Minister or Ministers, other interested parties and accountable authorities are provided with opportunity to comment on any matters reported. Where they choose to do so, their responses, or summaries thereof, are detailed within the reports.

The Auditor-General's Relationship with the Parliament and State Entities



2020 (No. 33)

2020
PARLIAMENT OF TASMANIA

Report of the Auditor-General No. 4 of 2020-21

Information and communications technology strategy, critical systems and investment

27 October 2020

Presented to both Houses of Parliament pursuant to
Section 23 of the *Audit Act 2008*

Auditor-General's reports and other reports published by the Office can be accessed via the Office's website. For further information please contact:

Tasmanian Audit Office

GPO Box 851
Hobart
TASMANIA 7001

Phone: (03) 6173 0900, Fax (03) 6173 0999
Email: admin@audit.tas.gov.au
Website: www.audit.tas.gov.au

ISBN: 978-0-6488176-4-2

Tasmanian Audit Office

Level 8, 144 Macquarie Street, Hobart, Tasmania, 7000
Postal Address: GPO Box 851, Hobart, Tasmania, 7001
Phone: 03 6173 0900 | Fax: 03 6173 0999
Email: admin@audit.tas.gov.au
Web: www.audit.tas.gov.au

27 October 2020

President, Legislative Council
Speaker, House of Assembly
Parliament House
HOBART TAS 7000

Dear Mr President, Madam Speaker

Report of the Auditor General No. 4 of 2020-21: Information and communications technology strategy, critical systems and investment

This report has been prepared consequent to examinations conducted under section 23 of the *Audit Act 2008*. The objective of the review was to express a reasonable assurance opinion on whether government information and communications technology (ICT) strategy, critical systems and investment are managed in an effective, coordinated and strategic manner.

Yours sincerely

[redacted]

Rod Whitehead
Auditor-General

Page left blank intentionally.

Table of contents

Independent assurance report

This independent assurance report is addressed to the President of the Legislative Council and the Speaker of the House of Assembly. It relates to my performance audit (audit) on the effectiveness of government ICT strategy, critical systems and investment.

Audit objective

The objective of this audit was to form a conclusion on whether government ICT strategy, critical systems and investment are managed in an effective, coordinated and strategic manner.

Audit scope

The audit examined and analysed information relating to government ICT strategy, critical systems and investment in the following agencies:

- Department of Premier and Cabinet (DPAC), including the Digital Strategy and Services (DSS) Division
- Department of Communities Tasmania
- Department of Education
- Department of Health (including the Tasmanian Health Service)
- Department of Justice
- Department of Police, Fire and Emergency Management
- Department of Primary Industries, Parks, Water and Environment
- Department of State Growth
- Department of Treasury and Finance (Treasury).

Although TasTAFE is represented in the whole-of-government[1] (WoG) bodies that comprise the government digital services governance framework, it was not included in the scope of this audit.

Audit approach

The audit was conducted in accordance with Australian Standard on Assurance Engagements ASAE 3500 *Performance Engagements* issued by the Australian Auditing and Assurance Standards Board, for the purpose of expressing a reasonable assurance conclusion.

The audit evaluated the following criteria:

1. Did the government have a strategic approach to ICT governance and decision making across the government that is coordinated and effective?

[1] Whole-of-government is limited to the Tasmanian General Government Sector. For the purposes of this audit references to WoG is limited to the agencies included in the scope of the audit.

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?

Audit observations and findings were based on information and evidence obtained through:

- examination of relevant documentation (agency processes, procedures, policies and plans)
- examination of relevant documentation pertaining to the governance framework
- examination of Structured Infrastructure Investment Review Process (SIIRP) investment proposals
- other ICT investment funding documentation
- interviews with key agency stakeholders and select personnel from DSS.

Responsibilities of management

Agencies are responsible for maintaining and implementing ICT strategies that support the management of critical systems vital for service delivery and securing funding required for ICT investment. DPAC is responsible for the facilitating WoG ICT governance and decision making.

Responsibilities of the Auditor-General

In the context of this audit, my responsibility was to express a reasonable assurance conclusion on government ICT strategy, critical systems and investment.

Independence and quality control

I have complied with the independence and other relevant ethical requirements relating to assurance engagements, and apply Auditing Standard ASQC 1 *Quality Control for Firms that Perform Audits and Reviews of Financial Reports and Other Financial Information, and Other Assurance Engagements* in undertaking this audit.

Conclusion

It is my conclusion government ICT strategy, critical systems and investment are not managed in an effective, coordinated and strategic manner, in terms of efficiency and effectiveness, with respect to certain criteria or sub-criteria of the performance audit.

This is because, despite the implementation of a digital governance and decision making framework, there is insufficient guidance to support whole of government ICT planning and prioritisation. Opportunities to develop shared ICT services, products or develop a whole of government ICT vision improving the efficiency and effectiveness of ICT delivery have not been realised. Agency ICT strategies and plans varied in quality and the lack of an ICT vision meant they could not align to government priorities. This further inhibited agencies ability to effectively plan for the replacement or upgrade of legacy systems critical for service delivery. Government decision making regarding ICT investment was also not informed by a whole of government vison and approach.

Rod Whitehead
Auditor-General

27 October 2020

Executive summary

Summary of findings

ICT underpins how a government delivers essential services effectively, efficiently and securely in today's society. It is vital ICT plans are delivered through effective ICT strategies, there is a clear understanding of critical systems and investment is targeted to achieve desired outcomes and improvements. These are fundamental considerations within the strategic planning processes of the government.

Our audit assesses how well the government sets out the vision and WoG approach for the future development of ICT and how this is supported by agency ICT strategy and planning which underpin the maintenance, investment and replacement of critical systems that are essential to service delivery.

To strengthen its strategic approach to ICT, in December 2011 the government issued the *Tasmanian Government ICT strategy*. This strategy aimed to drive improved and transformed service delivery, greater public sector productivity and informed decision making by enabling ICT resources that were forward-looking, adaptable and effectively managed across the public sector. However, following a change of government, elements of the strategy were not implemented and the uptake by agencies was limited. Consequently, we have not further considered the 2011 strategy during the course of this audit.

To further develop a WoG approach to digital capability, strategy and transformation, over the course of 2018 and 2019, a Digital and ICT governance framework (governance framework) was established, comprising three core bodies: the Digital Services Board (DSB); Deputy Secretaries Digital Services Committee (DSDSC); and the Digital Services Advisory Group (DSAG). Some aspects of this governance framework are working well. These included the recent development of policies relating to cybersecurity, the cloud and the release of a digital strategy, *Our Digital Future* (2020), outlining the government's approach to digital transformation. *Our Digital Future* outlines that a digital strategy should precede the development of an ICT vision and a plan to implement this vision.

It is acknowledged the scope and responsibilities of the governance framework and the above policy development are broader than just ICT as it encompasses a focus on digital capability, strategy and transformation of which ICT is a subset. Given the government's relatively recent progression towards digital strategy development and implementation, our audit was primarily focused on the more traditional elements of ICT strategy, management, governance and investment.

There are areas where the governance framework has yet to make significant progress. It has not delivered significant outcomes demonstrating effective service sharing, cost savings and productivity gains that could be achieved across WoG. Similarly it has not helped to identify duplication of effort that could be eliminated between agencies through a greater awareness of ICT service delivery requirements.

A key aspect limiting progress is the lack of a vision outlining the future development and priorities for ICT across WoG. There was also no evidence that the current WoG function,

currently delivered through DSS, has the appropriate mandate and resourcing to be able to support the delivery of a WoG ICT vision if one was developed.

There was no comprehensive information from agencies supporting the WoG framework and 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.

In our view, to achieve more effective WoG ICT governance and decision making a planned approach should be adopted and implemented. Such a plan should be defined by the government, and developed and executed within the next 18 months. This would support a comprehensive, informed vision across WoG. Agencies could then better plan for their own needs, increase collaboration for mutual gain and receive the benefits of a strategic WoG ICT focus.

Each agency has responsibility for its own ICT planning approach that links through to their Corporate Plan and underlying Branch plans. Generally, agencies can demonstrate a logical, systematic approach to ICT strategic planning and key asset management.

The limitations of the current WoG approach means planning is siloed within agencies and is variable, with differing levels of capability and maturity impacting on the quality of their strategies and plans. Guidance for agencies in developing plans was limited and, together with the absence of a WoG ICT vision, agencies were unable to plan for government priorities or realise effectiveness and efficiency improvements.

Our audit identified deficiencies in agencies ability to document and understand their current ICT environment and the management of long-term or high value key ICT asset replacement. This also impacts the development of a WoG ICT vision and strategy to prioritise the investment and replacement of these critical ICT assets.

Funding for ICT infrastructure projects is hampered by the lack of a WoG ICT vision. 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. This would provide more clarity regarding the evaluation and prioritisation of ICT investment.

As there is no strategic approach to prioritising departmental ICT investment proposals that could better inform and guide government and Budget decision making, the current Budget funding process is likely to only be effective for agencies which have the internal capability and capacity to complete a comprehensive Budget submission or SIIRP business case. Many agencies advised the low success rate of ICT Budget submissions for large scale, expensive ICT projects could influence their approach to preparing business cases for such projects. As a result, significantly aged and unsupported (by the vendor) ICT assets, or those at risk of failure, remain in operation with no real plan for replacement. An investment evaluation and prioritisation framework based on a WoG ICT vision would facilitate enhanced ICT investment decision making from a broader WoG perspective.

As a result of the above, there is a potential risk that critical ICT assets may fail due to an inability to adequately strategically plan, or obtain appropriate funding, for their replacement or investment needs. Large scale, long-term or high value ICT asset

replacement is at greater risk. As such, there is a possibility the government may not be able to deliver an essential service in the future.

Finally we found the development of agencies digital capability is at an early stage. Agencies were developing planned pathways to digital capabilities. This includes future delivery models, and potential efficiencies to be gained through shared services or business processing.

We would like to thank the agencies for their assistance in undertaking this audit.

Recommendations

1. The government enhance ICT investment evaluation and prioritisation by developing, through its current ICT framework, a WoG 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.
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
    d. critical assets that are significantly aged or at potential risk of failure.
3. The government review the terms of reference for the 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.
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.
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.
6. Treasury revisit the feedback approach for SIIRP submissions to better inform agencies on areas for improvement for future SIIRP submissions.
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.

Submissions and comments received

In accordance with section 30(2) of the *Audit Act 2008* (Audit Act), a copy of this Report was provided to the Secretary of each agency. A summary of findings or Report extract was provided to the Treasurer, and other persons who, in my opinion, had a special interest in the Report, with a request for submissions or comments.

Submissions and comments we receive are not subject to the audit nor the evidentiary standards required in reaching an audit conclusion. Responsibility for the accuracy, fairness and balance of these comments rests solely with those who provided the response. However, views expressed by the responders were considered in reaching audit conclusions.

Section 30(3) of the Act requires this Report include any submissions or comments made under section 30(2) or a fair summary of them. Submissions received are included in full below.

Minister for Science and Technology

The Tasmanian Government is focused on building strong foundations to support community wellbeing and digital inclusion, a vibrant digital economy and workforce, a range of Government services that are easy to access and straight-forward to use, and most importantly; ensuring the integrity and safety of Government held data.

The release of the state's inaugural strategy for digital industry and service transformation; *Our Digital Future*, is this roadmap towards an even more vibrant digital future for our State.

The Department of Premier and Cabinet's Digital Strategy and Services division has collaborated across multiple domains to develop the Government's first three-year strategy for digital transformation, which was drafted in consultation with all Government agencies and with significant input from the Department of Treasury and Finance and the Department of State Growth. I thank all Departments involved for their excellent work and I unequivocally support the Whole-of- Government response to this report which has the support of all Department Secretaries.

It is fair to say that it is a matter of regret that protracted and critical under-investment in crucial IT services and cyber security by previous State Governments has resulted in Tasmania historically trailing other jurisdictions.

Since coming to Government, we have focussed on building resilience in our cyber security capacity, which had previously left us considerably exposed - as previously identified in the Report of the Auditor-General No. 8 of 2014-15 - *Security of information and communications technology (ICT) infrastructure*. Since this publication, the Tasmanian Government, working in tandem with Departments and led by the Chief Information Officer have considerably enhanced our capabilities.

We know that digital maturity is developed incrementally. As the Government's first three-year strategy, *Our Digital Future* is the first step on that journey and working co-operatively and constructively with industry, we're committed to building additional capacity to see this vision fulfilled.

Relevant Ministers will discuss your report with their Departments in relation to the responses to recommendations. However, we will not be deterred from our necessary and deliberate focus on cyber security and our ongoing efforts in digital transformation, which will see more Government services available online for the benefit of Tasmanians who wish to use them.

The Honourable Michael Ferguson MP

Minister for Science and Technology

Collective response from Digital Services Board members

We acknowledge the findings of the ICT Strategy, Critical Systems and Investment Audit. As a State Service we are strongly committed to ensuring that we continue to meet the current and future needs of the Tasmanian community through the use of digital and information technologies. Department Secretaries through the Digital Services Board have provided comments below in relation to the audit recommendations but would like to take this opportunity to reiterate the initial feedback provided to the Audit Office, that a digital strategy and digital vision are necessary precursors to an ICT vision and ICT strategy.

The Government's Digital Strategy, Our Digital Future (www.digital.tas.gov.au), includes a key action to develop a technical roadmap that will articulate the Government's ICT strategy and ICT vision. The development of this Roadmap has commenced. It would be inappropriate for the Government to define an ICT strategy or vision in the absence of a digital vision and strategy.

The focus for Tasmanian Government and the Digital Services Board has appropriately been on digital transformation and cybersecurity. This includes protecting the data of Tasmanians and delivering new and improved digital services to citizens. The Digital Services Board consider digital transformation and cyber security are the appropriate priorities and are critical to inform and drive the technology roadmap rather than having technology drive the services of government. This audit however is primarily focused on ICT technical risks and related funding priorities and ignores risks and opportunities relating to the provision of secure and user-friendly digital services for Tasmanian businesses and communities.

The protection of data of Tasmanians held by the Government and ICT services are the priority for the Government and since the earlier *Security of information and communications technology (ICT) infrastructure* audit, there has been a sustained effort to enhance the Government's cybersecurity posture.

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

Strengthening cyber security, building digital culture and capability across government, adopting a cloud-first policy; enhancing identity and information management; and establishing common data sharing services are the enablers that the Government's digital transformation agenda is focussing on. Regrettably, these elements are inadequately considered in what this audit acknowledges as its primary focus: 'the more traditional elements of ICT'.

The following comments are provided in response to the audit recommendations:

Recommendations 1 and 2 (whole-of-government ICT vision and strategy)

The Government's view – acknowledged in the Report's 'Summary of findings' – is that a digital transformation strategy was a necessary precursor to setting ICT strategy direction.

Our Digital Future sets a broader strategic context for digital transformation – not only within government, but recognising digital opportunities to partner with and support Tasmanian businesses and communities. Better understanding the digital transformation

needed to provide ‘anytime, anywhere’ services to all Tasmanians is a critical first step before appropriate technology investments – and opportunities for agencies to leverage common platforms and procurements – can be identified.

Our Digital Future specifies the development of a whole-of-government technology roadmap as a strategic action and this body of work addresses Recommendations 1 and 2 and the timeframes will defined as part of this work.

Recommendations 3 and 4 (Digital Services Board)

The report suggests a failure in the WoG ICT governance and suggests that the Terms of Reference for the Digital Services Board be reviewed to ensure it has the mandate to better support a prioritised and collaborative approach to ICT across agencies and to provide support and guidance.

The Digital Services Board is of the opinion 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 and the role of the Digital Services Advisory Group and notes that a biennial review is already part of the Terms of Reference of each of these governance bodies.

Recommendation 5 (Agencies key ICT asset investment)

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.

Recommendation 6 (Treasury feedback on SIIRP submission)

The Department of Treasury and Finance will review its feedback and guidance to agencies seeking funding through the Structured Infrastructure Investment Review Process.

Recommendation 7 (Agency ICT critical asset registers)

Agencies agree to explore opportunities to build more consistent asset management practices.

Jenny Gale

Chair

Digital Services Board

1. Introduction

Context

1.1 ICT underpins how a government delivers public services efficiently and securely via agencies underlying ICT assets. Managing ICT strategy, critical systems and investment in an efficient, coordinated and strategic manner is essential in the delivery of services by the government now and into the future.

1.2 Agencies depend on ICT systems to deliver public services, efficiently and effectively manage operations and fulfil statutory obligations. These ICT systems may include single or multiple information technology (IT) applications.

1.3 In December 2011 the *Tasmanian Government ICT Strategy* (2011 ICT Strategy) was released. This strategy aimed to drive improved and transformed service delivery, greater public sector productivity and informed decision making by enabling ICT resources that were forward-looking, adaptable and effectively managed across the public sector. However, following a change of government, elements of the strategy were not implemented and uptake by the agencies was limited.

1.4 To drive the implementation of the ICT Strategy, DPAC, through the Office of eGovernment, was tasked with monitoring the progress of the ICT Strategy, advising on ICT investments, and developing benchmarks on ICT investments and performance across the WoG.

1.5 The government also established the ICT Policy Board, with its role being to provide advice to the Premier on strategic directions for ICT, including investment and performance of ICT. This was to be achieved through the coordination and consolidation of agency:

- strategic ICT plans
- ICT asset management plans
- ICT investment proposals.

1.6 In March 2019, the government took the following actions as part of its commitment to leveraging new and emerging technologies to support improved public policy decision making, service delivery and community outcomes:

(i) unified the resources of two former DPAC divisions, Office of eGovernment and Telecommunications Management Division (TMD), to establish a new division, DSS, with the mission of '*working together to lead the digital transformation of the government through the delivery of trusted advice, strategies and services*'

(ii) established new digital services governance framework at a WoG level, comprising three bodies with different levels of responsibility:

- DSB
- DSDSC
- DSAG.

1.7 DSB, DSDSC and DSAG constitute the core bodies within the governance framework. The Minister for Science and Technology (the Minister) has representation through DPAC.

1.8 Departmental IT committees are the agencies mechanism to feed points of interest into the governance framework. This information flow is both upward and downward.

1.9 Under the governance framework the Minister and DSB are to *'…agree on and regularly update a coherent strategy for digital services, information management, cybersecurity and ICT that supports delivery of the government's strategic priorities'*[2] into the agencies.

1.10 In October 2019, the government commenced public consultation on its Digital Transformation Strategy Package and subsequently received eleven external submissions. On 26 June 2020, *Our Digital Future* was released[3] by the Minister, detailing the government's vision and strategy for digital transformation.[4]

1.11 From an agency perspective the ability and method of managing ICT strategy, critical systems and investment varied considerably depending on the scale, resourcing, capability, geographic locations, history (whether agencies have experienced machinery of government[5] changes within the last five years), and structure (aspects of ICT inter-agency dependency or decentralised ICT).

1.12 The specific characteristics of each agency are a contributing factor explaining variations in outcomes of managing ICT strategy, critical systems and investment between agencies.

What is an ICT strategy and why is it important?

1.13 In this report we examine criteria relating to the government's ICT strategy and agency ICT Strategic Plans, and outline what these are and why they are important.

1.14 An ICT strategy is generally considered to set out the direction of how ICT will be used to assist a business deliver services or win in their chosen market. An ICT strategy sets the long-term strategic direction of an entity's technology capabilities.[6]

1.15 An ICT strategy is a critical component of an organisation's governance and planning process. It sets out a roadmap of how an entity will move from the current state to the future state by defining critical projects and initiatives to be delivered, and the

---

[2] Source: Extracted from the 'Governance and reporting relationships' table contained in the *Digital Services Board Terms of reference 1.0 (Approved: 30 October 2018)*.

[3] *Our Digital Future* is dated March 2020, but was formally released on 26 June 2020

[4] Source: Department of Premier and Cabinet website

[5] A machinery of government change occurs when the government decides to change the way administrative responsibilities are managed. It can involve the movement of functions, resources and people from one department or agency to another, and may be effected through the establishment, abolition or merger of agencies.

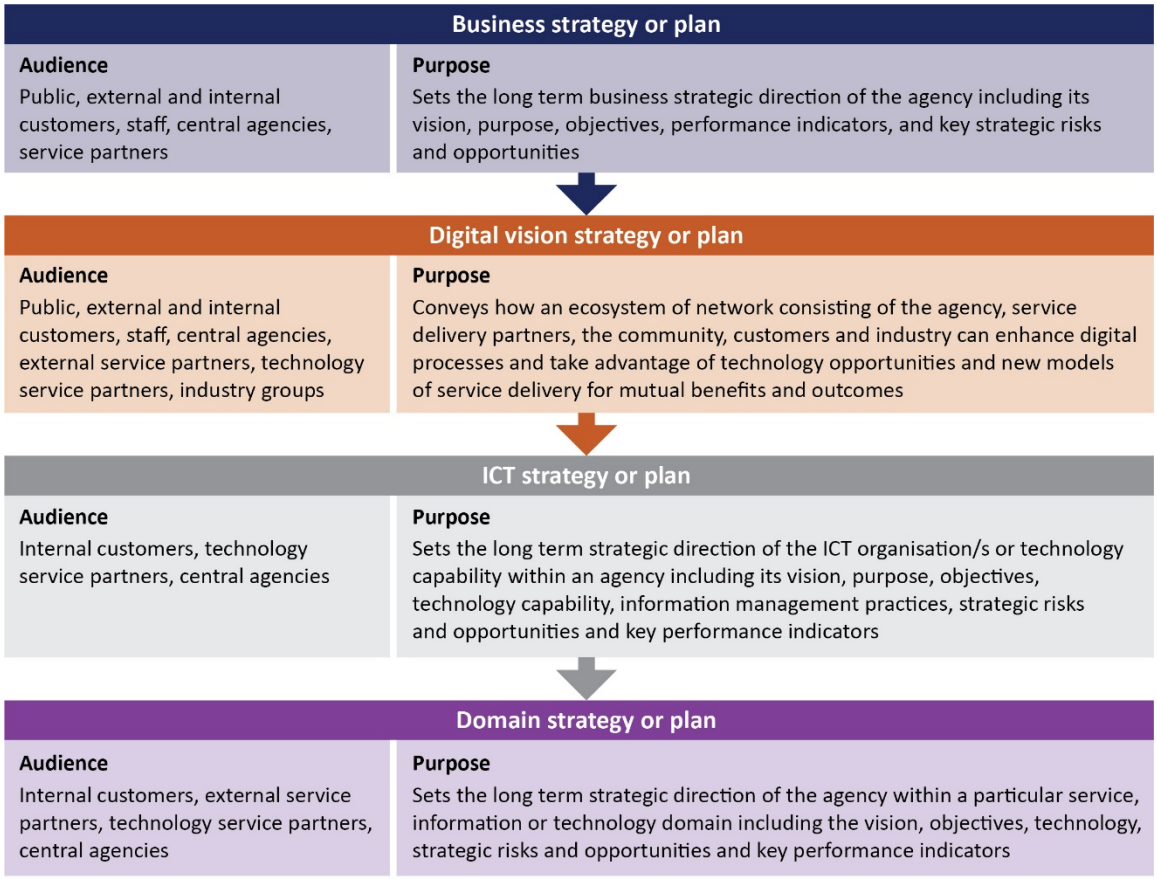
[6] Source: Queensland government at qgcio.qld.gov.au

timeframe for doing so. Benefits it expects to obtain and the risks to achieving the desired outcomes are also central components of the strategy.

1.16 The importance of the ICT strategy is that it defines how the ICT components of the Corporate Plan will be delivered. The intent is on long-term planning, and as such, a three to five year period allows time for plans to be put in place and actioned through the lifecycle of the strategy. An annual review of actions or progress will ensure planning remains up-to-date and relevant.

1.17 An example of how the ICT strategy interacts with other components within the overall governance and planning process for an entity is displayed below in Figure 1.

Figure 1: Hierarchy of business, digital or ICT related strategies or plans



Source: Queensland Government

1.18 As detailed in Figure 1, the Corporate or Business Plan sets the overall direction, vision and objectives for an organisation. A Digital Strategic Plan sets a broad vision encompassing both an internal and external focus for business services and new strategic opportunities. The ICT Strategy is an internal strategy that should have clear links to the Digital Strategic Plan and Corporate Plan.

1.19 A traditional ICT strategy is the long-term planning and implementation of strategic technology capability, in its various forms, to enable the delivery of business services. This includes the service model delivery of the corporate vision, objectives, service delivery capability, strategic risks, information management processes, key performance indicators (KPI's) and investment planning.

1.20 A Digital Strategic Plan is the transformation of traditional services using technology or through new business models using new channels and opportunities. Multiple factors can be drivers of this transformation including partnered service delivery model changes, technology opportunities, public and internal and external user expectations. The desired outcome is greater efficiencies within digitised service models with a beneficial effect on all users.

What are key ICT assets?

1.21 Key ICT assets are those assets or systems identified by an agency as vital to the delivery of services, without them, the agency would be unable to deliver essential services.

1.22 This audit focussed on IT applications, single or multiple, which were key in the delivery of services from each of the agencies but did not include hardware.

What do we mean by a WoG ICT vision?

1.23 A WoG ICT vision is a plan to deliver beneficial, coordinated and measurable short, medium and long-term WoG information. It should communicate technology outcomes. These should support the strategic ICT direction as defined by the government. Broadly, the focus is on ICT priorities such as productivity and efficiency gains, removal of duplication, optimising shared services. It should also address key asset needs (immediate and future), collaboration, enhanced information flow, capability development and initiatives to achieve productivity and cost efficiencies across agencies.

The 2011 Tasmanian Government ICT Strategy

1.24 The 2011 ICT Strategy was approved by the then government in December 2011 with the aim of driving improved and transformed service delivery, greater public sector productivity and informed decision making in relation to ICT.[7] This was to be enabled by planning, investing and monitoring a strategic approach to ICT across the government.

1.25 The 2011 ICT Strategy had five key objectives[8]:

(i) improved productivity in the public sector through investment in ICT

(ii) improved and transformed service delivery which is more client centric and more integrated across government, through ICT

(iii) better access to information for the community, business and public sector employees

(iv) strong leadership, focused investment decisions and effective management of ICT across the public sector

(v) a common approach to the provision of commodity ICT resources.

---

[7] 2011 *Tasmanian Government ICT Strategy*

[8] 2011 *Tasmanian Government ICT Strategy*

1.26 Agencies uptake of the 2011 ICT strategy varied significantly, with a limited number incorporating aspects into their ICT Strategic Plans and others seemingly not considering it at all. This strategy has not been subsequently updated. As a result the 2011 ICT Strategy has not been reviewed by this audit.

1.27 There was no evidence of a current government ICT Strategy in operation.

Our Digital Future

1.28 *Our Digital Future* defines a vision and strategy for digital transformation across government, the community and the economy, and outlines a direction, principles and major actions for each as shown in Table 1 below.

Table 1 Direction, principles and major actions

	Digital government	Digital Community	Digital Economy
Direction	The community is best served by a progressive government that puts the needs and expectations of citizens first, transforming the way it works and delivers services.	Equal opportunity to interact with digital services and information in easy to use, convenient and readily available ways.	Bolster the economy by the competitive advantage, productivity growth and prosperity enabled by knowledge-driven digital transformation.
Principles	Simplicity Security Strategy	Accessibility Ability Affordability	Capability Creativity Connectivity
Major actions	Eight major actions identified including developing a whole-of-government technology roadmap, adopting a Cloud[9] first policy, prioritising critical asset protection from a cybersecurity perspective, and developing digital culture and capability across government departments.	Six major actions identified including supporting digitally disadvantaged groups, strengthening lifelong digital skills learning and increasing 'smart city' technology.	Six major actions identified including empowering local business, promoting digital education and supporting technology start-ups and capabilities.

Source: *Our Digital Future* (March 2020)

Our Digital Future's goal is '*to develop stronger foundations to support 'anytime, anywhere' services and information'*.[10]

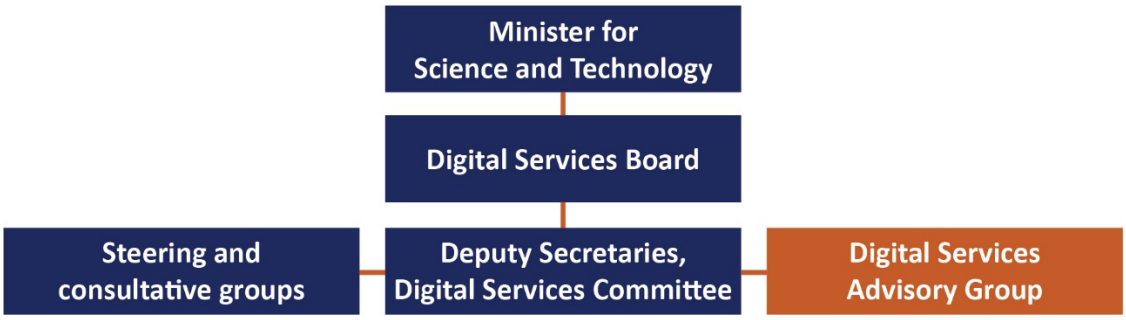
[9] Networked computing facilities providing remote data storage and processing services via the Internet

[10] Source: *Our Digital Future* (March 2020)

The current ICT structure, roles and responsibilities

1.29 DSB, DSDSC and DSAG constitute the core bodies within the governance framework, with the relationship between the bodies illustrated in Figure 2.

Figure 2: Government ICT framework



Source: DSB Terms of reference (30 October 2018)

1.30 The Minister is to provide DSB with direction through an agreed statement of direction for digital services, information management, cybersecurity and ICT across government, and endorsement of government policies for digital services, information management, cybersecurity and ICT. The Minister and DSB agree on, and regularly update, a coherent strategy for digital services, information management, cybersecurity and ICT that supports delivery of the government's strategic priorities.[11]

1.31 The role of DSB is to consider, champion and support investment in the implementation of digital strategies, policies and initiatives with WoG benefits. DSB is responsible for approval of strategies and policies, and delegates other responsibilities for standards, projects and services to the DSDSC. DSB is chaired by the Secretary of DPAC and includes appointed or acting Secretaries of departments and the TasTAFE Chief Executive Officer.[12]

1.32 The role of DSDSC is to support, execute delegated responsibilities and provide collective agency advice and recommendations to DSB in relation to digital strategies, policies, performance and investment. DSDSC is chaired by the Government Services Deputy Secretary in DPAC, and includes relevant Deputy Secretaries or equivalents from departments and TasTAFE. DSDSC may establish steering or consultative groups as required.[13]

1.33 The role of DSAG is to support and provide collective advice and recommendations to DSDSC in relation to digital strategies, policies, performance and investment. Members comprise Chief Information Officers (CIO) or equivalents from departments and TasTAFE and is chaired by the government CIO who is also responsible for the operation of DSS within DPAC.[14]

---

[11] *DSB Terms of reference* (30 October 2018)

[12] *DSB Terms of reference* (30 October 2018)

[13] *DSDSC Terms of reference* (30 October 2018)

[14] *DSAG Terms of reference* (30 October 2018)

1.34 The key responsibilities of DSB, DSDSC and DSAG are split across the following five key areas:

- digital strategy and policy
- WoG project portfolio
- cybersecurity
- information management and data analytics
- digital capability development.

1.35 The responsibility matrix contained in the respective terms of reference across the WoG framework is shown in Table 2 below.

Table 2: Responsibility matrix

Governance level	WoG issues, solutions and initiatives				
	Digital strategies	Digital policies	Digital standards	Digital projects	Digital services
Digital Services Board	Create and approve	Create and approve	Delegated to DSDSC	Delegated to DSDSC	Delegated to DSDSC
Deputy Services Digital Services Committee	Endorse	Endorse	Create and approve	Create and approve	Create and approve
Digital Services Advisory Group	Endorse	Endorse	Endorse	Consulted	Consulted

Source: DSB Terms of Reference (30 October 2018)

1.36 The role of DSS 'brings together policy, project management and service delivery capability to strengthen strategic partnerships across all agencies and industry providers'.[15]

1.37 DSS operates under the same organisational, statutory and policy frameworks as other DPAC divisions. The CIO operates under DPAC with a WoG role and also acts as Chair of the DSAG.

1.38 Agencies are responsible for creating and implementing their own ICT strategies, governance and investment decisions. Funding for ICT investment however, is obtained through various avenues including the Budget submissions, Australian

[15] The role of DSS is defined on its website www.dpac.tas.gov.au/divisions/digital_strategy_and_services

Government funding and internal funding (including sale of assets and funding reallocations).

Recent government investment in digital transformation projects

1.39 In May 2017, the government recognised the importance of investment in key digital transformation projects by announcing a $61.9 million Digital Transformation Priority Expenditure Program in the 2017-18 Budget.

1.40 In the first year of the program, $52.5 million, representing 84.8% of the available funding under the program, was allocated to the following projects:

- Department of Health and Human Services (now Department of Communities Tasmania) - upgrade of the Child Protection Information System, $6.0 million
- Department of Health and Human Services (now Department of Health) - Health ICT Priority Infrastructure Program, $18.0 million
- Department of Justice - Justice Connect project aimed at delivering 'a contemporary, integrated, end-to-end Justice System' by addressing shortcomings with existing systems, integration, processes and data supporting the criminal, correctional and civil jurisdictions, $16.6 million
- Department of Police, Fire and Emergency Management - Project Unify with the aim of replacing the agency's Information Data Management System and several other legacy systems, $11.9 million.

Impact of COVID-19

1.41 On 30 January 2020, the spread of coronavirus 2019 (COVID-19) was declared a Public Health Emergency of International Concern by the World Health Organisation (WHO). Subsequently, on 11 March 2020, the WHO declared COVID-19 a pandemic.

1.42 The rapid onset of COVID-19 created an environment in which all agencies had to adapt quickly to ensure continuity of service delivery and compliance with workplace health and safety requirements. The government and agencies response to the pandemic from an ICT perspective is not within the scope of this audit.

2. Does the government have a strategic approach to ICT governance and decision making across the government that is coordinated and effective?

In this Chapter we assess the effectiveness of the government's strategic and coordinated approach to decision making related to ICT by determining whether the governance and decision-making framework:

- had been defined to support WoG ICT planning and identification of ICT priorities (short, medium and long-term)
- supported collaboration for common ICT policy, and where possible shared products, services and resources at a WoG level
- provided prioritised operational, development and strategic function goals.

Chapter summary

A governance and decision making framework has been established and is providing a pathway for agencies to raise ICT points of relevance or concern. Regular meetings across the bodies within the governance framework have resulted in policy development in key areas such as cybersecurity, cloud and the release of *Our Digital Future*.

There has not been sufficient guidance from the government to support WoG ICT planning and prioritisation across agencies over the short, medium and long-term because there was no current government WoG ICT vision. While *Our Digital Future Strategic Action Plan* acknowledges the need to develop a WoG technology roadmap amongst other WoG aspects, it cited the roadmap as 'to be started'.[16]

Agencies are responsible for their ICT planning and have not received broader WoG guidance from the government. To date, there have been two WoG ICT policies agencies have interpreted, implemented and internally funded.

We found collaboration does exist, and while the government may know about shared ICT services anecdotally, the full extent of collaboration across all agencies was not formally linked to a strategic and coordinated approach.

DSB's terms of reference and the lack of a government WoG ICT vision limit the effectiveness of the governance framework in providing prioritised operational, development and strategic function goals. Clarity of direction through a WoG ICT vision and a change to the DSB's terms of reference will enable the governance framework to better promote coordinated and effective governance and decision making and deliver beneficial outcomes across the WoG.

[16] Source: *Our Digital Future Strategic Action Plan* May 2020

To develop a WoG ICT vision, the government needs to collect better quality information from all agencies. This would enable it to formulate an informed and comprehensive ICT vision across WoG, including identifying ICT priorities. Decision making could then be based on a comprehensive assessment of agencies ICT environments, projects and future needs, consider collaborative shared solutions and set strategic goals.

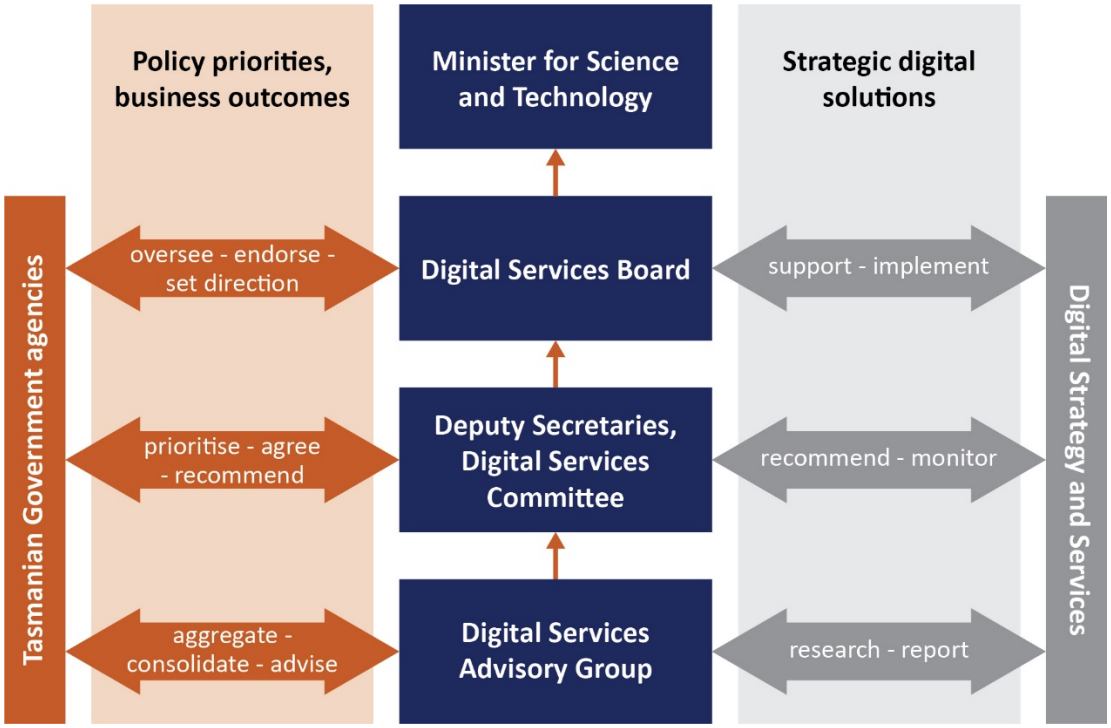
Under the current framework, and without an informed WoG ICT vision, potential efficiencies, productivity gains and cost savings are less likely to be realised.

A governance and decision making framework has been established and is providing a pathway for agencies to raise ICT points of relevance or concern

2.1 The governance framework and the core bodies within it (DSB, DSDSC and DSAG) were outlined in Section 1 of this Report.

2.2 The level of inter-reliance across the governance framework is demonstrated in Figure 3.

Figure 3: Inter-reliance across the government ICT framework



Source: "DSS 2021 A two-year strategic plan for Digital Strategy and Services" (Draft)

2.3 IT committees are the mechanism for agencies to share ICT points of relevance or concern with the core bodies of the governance framework. This information flow is both upward and downward.

2.4 Membership across the core bodies was sourced from the agencies, providing another avenue for agencies to exchange relevant ICT related information.

2.5 Our audit identified agencies were adopting the suggested government policies, with key policies driven by the government since the establishment of the governance framework being cybersecurity, the cloud, and the release of *Our Digital Future.*

2.6 We noted agencies actively participate in the core bodies that make up the governance framework. Although, due to capability and resource constraints, we identified a small number of agencies had limited ability to be able to fully participate in the governance and decision making framework.

2.7 Two agencies advised us their implementation of key policies was impeded by challenges in finding suitable resources and a lack of application guidance from the government.

There has not yet been sufficient guidance from the government to support WoG ICT planning and prioritisation over the short, medium and long-term

2.8 Underpinning the governance framework is the requirement of the government to provide ICT planning and identification of priorities. With the establishment of the governance framework over the last few years, we noted that this had not been actioned and there was no overarching WoG ICT vision or priorities provided to agencies at the time of our audit work. As a result, agencies did not have information available to facilitate a more informed and consistent approach to decision making, planning and prioritisation over the short, medium and long-term.

2.9 Agencies are responsible for their own ICT planning including service delivery, internal accounting, and administrative solutions. The application of the two WoG ICT policies mentioned above (cybersecurity and the cloud) required the agencies to separately interpret, implement and internally fund them, thereby creating duplication of functions and solutions across the sector.

2.10 We would expect to see a WoG ICT vision that sets out the key priorities for the government over the short, medium and long-term. Without the long-term WoG ICT vision of government ICT priorities, the ability to also plan across WoG was constrained.

2.11 While *Our Digital Future Strategic Action Plan* acknowledges the need to develop a WoG technology roadmap amongst other WoG aspects, it cited the roadmap as 'to be started'.[17]

[17] Source: *Our Digital Future Strategic Action Plan* May 2020

The governance and decision-making framework has not fully supported the implementation of shared services/products or common ICT policy at a WoG level

2.12 The ability of the government to support collaboration for common ICT policy, shared products and services was constrained as there was limited understanding of the shared services and ICT environments, capabilities, projects and needs of the agencies.

2.13 Through our audit work we identified most agencies provide shared ICT services to other agencies. The government does not have full visibility of these services. It may know about shared services anecdotally but the full extent across all agencies was not formally linked to a strategic, coordinated approach across the WoG. Formalisation of inter-departmental deliverables through service level agreements (SLAs) would allow for resource budgeting, provide greater visibility of usage and reliance, and enhance service accountability.

2.14 Greater visibility of agency ICT environments, capabilities, projects and needs at the government level is integral to the development of informed ICT guidance that could facilitate increased collaboration or sharing arrangements. Without this greater visibility the government cannot effectively plan for or promote enhanced collaboration across the WoG.

2.15 Funding for shared ICT service/products and common policy is considered in more detail in Section 5 of this Report. However, the funding of the core bodies within and administering the governance framework itself is also important. DSB, DSDSC, DSAG are not separately funded and are largely made up of representatives from agencies and are therefore indirectly funded by them. DSS is funded for specialised tasks (i.e. cybersecurity) and by agency contributions for shared services but other WoG projects are not funded or must be funded via Budget submissions. This results in DSS competing with the agencies it is supposed to support for ICT funding which is unlikely to promote collaboration.

DSB's terms of reference and the lack of WoG ICT vision limit the effectiveness of the governance framework in providing prioritised operational, development and strategic function goals

2.16 DSB's Terms of Reference were approved on 30 October 2018. The Terms of Reference define its role, which is to consider, champion and support investment in the implementation of digital strategies, policies and initiatives with WoG benefits.

2.17 The terms of reference are limited in that they only encourage DSB to 'consider opportunities or issues that may benefit from a WoG approach, and establish and oversee such an approach'.[18]

2.18 Policy advice issued by DSB under the governance framework was defined as either 'general' or 'essential'. Agencies had to consider general policy advice (which is only issued to assist agencies managing certain ICT aspects) and could choose to opt in or out of essential policy (which is only issued in compelling situations requiring consistent policy).

2.19 Table 3 below shows a matrix for the advice provided under the governance framework.

Table 3: Advice issued under the governance framework

Category	Rationale	Authorisation	Agency responsibility
General policy advice	To assist departments and TasTAFE with managing digital services, information management, cybersecurity and agency-based ICT resources more effectively and efficiently.	Board approval	Departments and TasTAFE are expected to seriously consider the applicability/ implementation of advice provided, according to specific circumstances.
Essential policy advice	Only used in situations that demonstrate compelling reasons for departments and TasTAFE to apply/ implement consistent policy.	Board approval with formal notification provided by the Chair to Heads of Departments and TasTAFE CEO.	Departments and TasTAFE are required to consider the advice and notify the Chair within two calendar months, either: • agreement to apply/implement the advice, and the expected timeframe; or • notification that the advice will not be applied/ implemented, including the rationale for that decision.

Source: DSB Terms of reference (30 October 2018)

[18] DSB Terms of reference (30 October 2018)

We found that agencies followed general policy advice and did not observe any cases where they had chosen to opt out of essential policy advice. Our discussions revealed this was influenced by pre-emptive strategic consultation from DSS.

2.20 With a WoG ICT vision outlining targeted cost efficiency gains, increased productivity and removal of duplication strategies, common agency functions could be delivered via shared ICT services. To achieve the desired outcome of prioritised and strategic goal setting, DSB could be tasked with the responsibility of delivering the cost efficiency gains, increased productivity and removal of duplication across agencies. This would require a change to DSB's Terms of Reference from 'consider' to 'deliver'.

2.21 Once a WoG ICT vision is defined by the government, DSB could support this with essential policy advice for critical ICT priorities across the WoG that can take away from agencies non-essential service delivery functions where benefits can be realised. Agencies could retain a high level of autonomy and focus on their critical service delivery, while receiving the outcomes of beneficial WoG priority implementation.

2.22 The existing DSB Terms of Reference and the lack of a WoG ICT vision limit the effectiveness of the governance framework to set prioritised operational, development and strategic function goals. As a result potential efficiencies and cost savings are less likely to be realised.

3. Had agencies prepared and maintained contemporary ICT Strategic Plans?

In this Chapter we assess whether agencies had prepared and maintained contemporary ICT Strategic Plans by determining whether:

- the ICT strategy was defined and aligned to both the broader business direction of the agency and government priorities
- the business and ICT objectives, risks, outcomes and benefits, including key performance indicators, were identified in the ICT strategy
- ICT strategy implementation options included capabilities, achievement of objectives and identification of outcomes or benefits
- the ICT strategy was monitored and periodically reviewed
- ICT plans were prioritised (short, medium and long-term) with associated risk and contingency plans reviewed.

Chapter summary

ICT Strategic Plans are the responsibility of each agency and the plans reviewed varied significantly in content and maturity. It was apparent there had not been a standardised approach provided to, or adopted by, agencies.

Agency ICT Strategic Plans were:

- generally aligned with broader business direction of the agency
- not able to be aligned with current government priorities, as these had not been articulated to the agencies
- lacked future planning for large investment requirements and/or adaption to alternative operating models.

ICT Strategic Plans broadly identified objectives, risks, benefits and outcomes but it was evident not all plans were subject to periodic review.

ICT Strategic Plans identified prioritised initiatives/projects over their term but risks potentially preventing the achievement of those initiatives were not consistently identified. By not adequately considering and preparing for key risks, agencies may be slow to react, likely to suffer longer and more costly issues, and face an increased risk of ICT project failure.

Key improvements identified were:

- increased standardisation or minimum content specification for ICT Strategic Plans
- better consideration of risks
- more frequent review of ICT Strategic Plans to ensure they remain up-to-date and relevant to the agency and its objectives

We observed, for most agencies, there was capacity to improve in one or more of these areas.

ICT Strategic Plans prepared by agencies varied significantly in content and maturity

3.1 Setting ICT strategy is the responsibility of each agency. We examined, where available, the ICT strategic planning documentation for the nine agencies within scope. We found:

- four agencies had current ICT Strategic Plans
- three agencies had ICT Strategic Plans that were in draft form, outdated, or unapproved, but there was evidence of ICT planning activities occurring in all cases
- one agency had a transition plan
- one agency did not have a documented strategy, although through inspection of documentation provided, we noted a coordinated approach to ICT planning was still evident as was progress towards enhancing their formal planning activities.

3.2 Of the seven ICT Strategic Plans and one transition plan reviewed, seven showed the ICT planning was embedded within a governance environment and demonstrated linkages, of varying degrees, between the ICT Strategic Plan and the Corporate Plan.

3.3 The level of planning maturity observed was diverse. One agency had developed an IT Strategic Plan using a Gartner model for the management of its business applications based on a four stage process. The agencies IT services section conducted a review process every 12 months to ensure management of business application, plan maintenance and investment were up-to-date. This process fed into a cost analysis to identify a 'make or buy' strategy for each business application. This agency demonstrated an ability to identify strategic direction at the organisational level that was able to seamlessly cascade to various initiatives at the operational level. Other agency plans were based off risk assessments, with current and future state assessments, prioritised projects and timelines. At the other end of the scale, one ICT Strategic Plan was very brief and lacked basic detail, and as noted above, one agency did not have an ICT Strategic Plan at all.

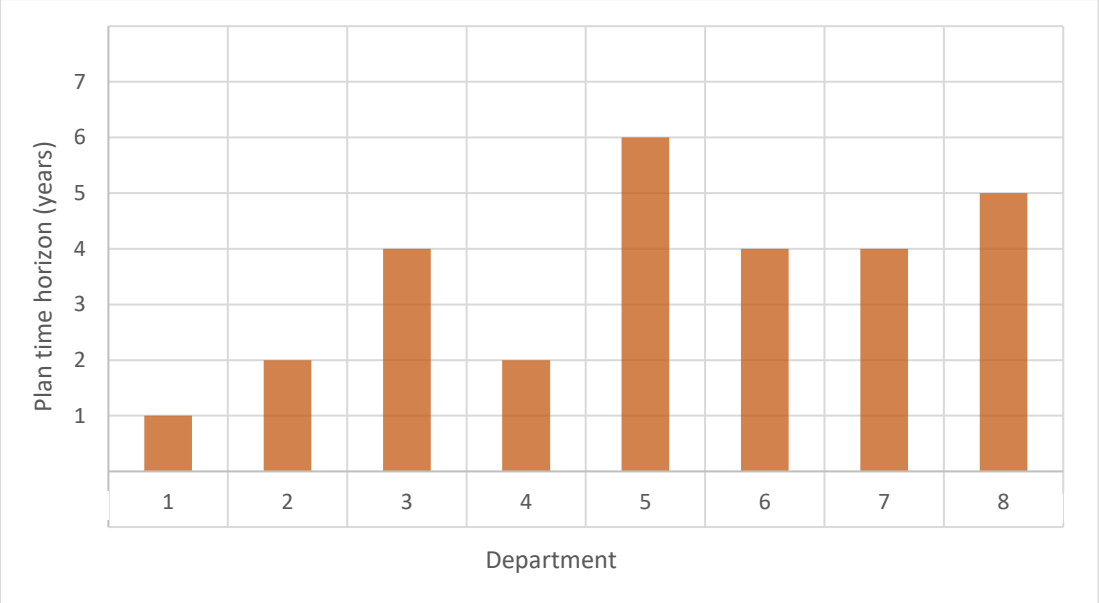
3.4 For the agency without an ICT Strategic Plan, the challenges in recruiting a stable ICT leader had inhibited their ability to develop a strategic vision. Despite the absence of leadership and key resources, which affected their ability to strategically plan and actively participate in the governance framework, it was demonstrated staff had attempted to carry forward critical ICT actions nominated by the most recent CIO.

3.5 The role of ICT within agencies in responding to machinery of government changes had challenged their ability to strategically plan for better ICT outcomes. For more recent machinery of government changes, agencies had prepared ICT transition plans. In one case, an agency used a merger to consolidate solutions. In another case, despite the implementation of the transition plan, the agency was reliant on other

agencies functionality and resourcing. These transition plans were vital to the ongoing provision of essential services and were not foreseen in the initial ICT Strategic Plan. It was evident machinery of government changes required significant time to facilitate and implement required ICT changes and significantly affected agencies ability to resource and plan for future ICT requirements.

3.6 The time horizon of the plans across the eight agencies with ICT Strategic Plans (or transition plan) varied from 12 months to more than six years, as summarised in Figure 4. Five of the eight plans have a time span of three to five years or more and the median length was four years.

Figure 4: Time horizon of ICT strategies.



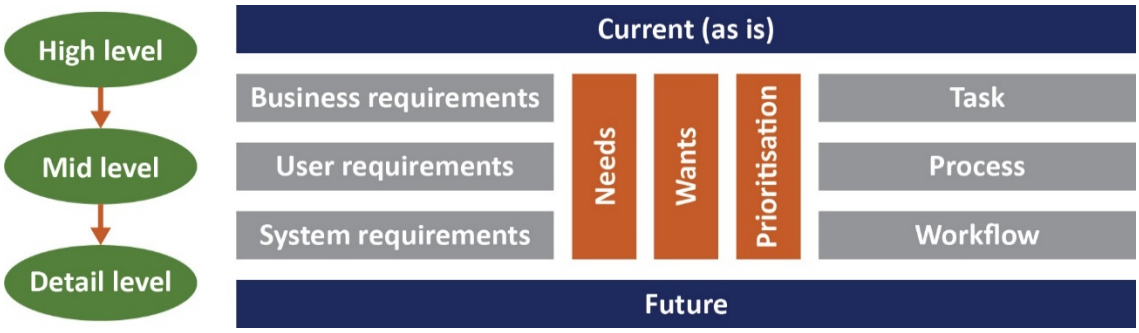
Source: TAO

3.7 There was significant variation in the level of detail and maturity within the ICT Strategic Plans. There had not been a standardised approach provided to agencies. A predefined, common approach could provide direction in terms of minimal or mandated content, promote consistency and comparability while maintaining sufficient autonomy for agencies to align the ICT Strategic Plan with the Corporate Plan and to responding to any specific agency circumstances.

3.8 Assessment of ICT Strategic Plans revealed there was limited visibility of the current state of ICT environments at the agency and WoG level. To plan, prioritise and transition to a target state it is essential to have an understanding of the current state. With visibility of each agencies current state, their planned maintenance, projects and investment, the WoG function could promote greater collaboration between agencies further driving the standardisation of solutions, sharing of costs and assisting in the uplift of ICT services in smaller agencies.

3.9 An overview of the assessment processes used to determine an agency's current state is illustrated in Figure 5.

Figure 5: Overview of Current State Assessment



Source: Deloitte

3.10 The lack of visibility of the current state of ICT environments and insufficient planning has led to:

- some agencies undertaking work required without planning the associated internal costs
- some agencies initiate projects in a reactive manner and do not have them documented in the current (or expired) ICT Strategic Plan
- the continued use of aged infrastructure.

Agency ICT Strategic Plans were not aligned with current government priorities as the WoG ICT vision has not been defined or articulated to the agencies

3.11 The incorporation of WoG policy, essential and general, into ICT strategy is the responsibility of agencies. Generally, the adoption of policy was followed by agencies and WoG policies (such as cybersecurity and the cloud) were considered in ICT plans. However, similar to the level of maturity noted above, the accompanying level of detail varied considerably across agencies.

3.12 Currently, the government has not set a vision across the WoG. The recent focus has been limited to the establishment of the governance framework. Some policy aspects have been considered and issued (for example, purchasing for Office 365 and the telephony platform for all agencies) current WoG priorities have not.

3.13 Although the governance framework had progressed, the government had not yet set a specific WoG ICT vision and associated priorities across the WoG. As a result, agencies were unable to reflect current WoG priorities in ICT planning.

ICT Strategic Plans broadly identified objectives, risks, benefits and outcomes, however it was evident these were not necessarily reviewed

3.14 While ICT Strategic Plans generally set out objectives, risks, outcomes and benefits expected from the successful execution of ICT planning, the outcomes and benefits were not reviewed on a regular basis. Given the number of expired plans in place it

was clear the objectives were also not regularly reviewed to reflect changing business needs, citizen expectations, technology, service delivery models and outcomes of funding requests.

3.15 For the agencies that were able to provide a contemporary ICT Strategic Plan, outcomes and benefits were identified either at the strategy level or at the initiative/project level.

3.16 The risk associated with the lack of timely review is ICT Strategic Plans become outdated or lose relevance and are no longer an integral part of the agencies' planning process.

3.17 Agencies identified and monitored the performance of core ICT services at the time of plan setting/revision and then tended to track the performance of ICT projects against project delivery metrics such as time, cost and completion status. The maturity of the agency ICT environment and resourcing had an impact on their capacity to monitor outcomes. Structured reporting channels and enhanced monitoring of ICT project outcomes and measurement against pre-defined KPI's or measurable project benefit outcomes could enhance the efficiency and effectiveness of ICT Strategic Plans.

3.18 Documentation provided by agencies showed different reporting formats and variations in relation to reporting on ICT projects and initiatives driven by them. There was often no clear correlation between the ICT Strategic Plan and the project reporting.

3.19 In line with the ICT Strategic Plan, a review of the initiatives should be undertaken during each 12 month period, including adjustment and reprioritisation if required. This would ensure plans remained relevant and aligned with the changing needs of the agency.

3.20 Where KPI's were reported these were not consistently defined or monitored. ICT strategies lacking clearly defined KPI's and measurable outcomes can result in poor monitoring and progression of objectives. The risks that arise are:

- projects running over budget
- issues/challenges not understood and replicated on future projects
- poor management of associated risks.

3.21 Agencies should plan, prepare and maintain ICT Strategic Plans with a minimum of a three to five year life cycle. At present, four agencies do not have a current ICT Strategic Plan in operation; this made up of one expired ICT Strategic Plan that is still being used, one unapproved (and expired), one in draft form, and one not having an ICT Strategic Plan. Preparation of rolling plans should be in place to prevent outdated ICT strategies. Agencies should gather the required ICT strategy information from the Corporate Plan (including the mission, objectives, strategy, strategic risks), relevant agency centralised functions and relevant branch/business units.

3.22 Information should flow top down and bottom up for clear visibility of an agencies plan and the underlying business units/branches responsible for strategy elements. ICT defined plans and initiatives should be reviewed annually with adjustments or updates applied to the ICT Strategic Plan to reflect the current environment and

progress. Initiatives completed should have a post implementation review in order to capture the achievement and identify opportunities for improvement in future ICT Strategic Plans.

Prioritised initiatives/projects were documented across the term of the ICT Strategic Plans however, risks potentially preventing the achievement of those initiatives were not consistently identified across agencies

3.23 To be able to prioritise initiatives/projects within their ICT Strategic Plan, an agency must first understand the current state of their ICT environment and determine a well-defined target state. Key initiatives/projects over the term of the plan are those that will move the agency from the current state to the desired state.

3.24 All eight ICT Strategic Plans (including the one ICT transition plan) contained details specifying key ICT projects or initiatives and a corresponding timeframe for implementation or achievement of objectives. However, the level of detail and clarity relating to prioritisation varied significantly.

3.25 Some plans did not identify risks that may prevent the successful execution of the identified projects or initiatives, while other plans (correctly) included risks that were not controllable by the agencies, for example, project funding.

3.26 Few agencies maintained an up-to-date ICT risk register that could form a central part of the ICT planning process. While some of the ICT Strategic Plans did consider common risk areas such as ICT outages and continuity, cybersecurity risk and ICT application support, there was limited evidence to demonstrate the assessment of risks to the ICT Strategic Plan and how these risks were to be managed to ensure the ICT Strategic Plan and initiatives were delivered. We found no evidence of agencies considering WoG specific risks.

3.27 The use of ICT risk registers, incorporating the results of a risk analysis focussed on ICT and documenting identified risks, cause, probability of occurrence and consequences, together with the a response plan, should form part of the ICT governance process for agencies.

3.28 The management of the ICT priorities for many agencies was mainly reactive. For example, the upgrade path of a website's software had not been maintained and in 2018 this website had to be taken offline due to cybersecurity vulnerability. The agency failed to effectively evaluate the risks and respond appropriately to them.

3.29 Most agencies acknowledged the need to better coordinate risk management and investment identification in line with associated risks or contingency planning for the medium and long-term.

3.30 By not adequately considering and preparing mitigations for key ICT risks, agencies will be exposed to challenging and costly ICT issues and an increased risk of ICT project failure.

4. Have agencies managed key ICT assets that are vital for service delivery effectively?

In this Chapter we assessed if agencies were managing key ICT assets that are vital for service delivery effectively by determining whether:

- agencies had appropriately identified key ICT assets
- key ICT assets were identified within ICT planning on a risk, contingency basis for replacement, upgrade or renewal
- agencies had adequately planned for the funding of key ICT assets that are due for replacement or renewal in the near future.

Chapter summary

Agencies identified key ICT assets vital for service delivery although the quality of documentation varied. Cross-agency reliance on ICT systems and/or resourcing was not documented or structured through SLAs. As a result, agencies could unintentionally adversely impact another agency's ability to provide essential services.

Short, medium and long-term planning for key ICT assets was included within ICT Strategic Plans. However, there was room for improvement in planning for the upgrade, renewal or replacement of long-term and high value ICT assets.

Funding for short-term replacement or renewal was considered but longer term funding for significant ICT key asset replacement, renewal, or transformational projects was difficult to plan for and obtain.

Long-term planning for some key ICT asset replacement was not sufficient. In several critical service delivery agencies aged infrastructure of 25 years or more was identified. As a result, there is potential for key ICT assets failing, leading to an inability to deliver essential services.

Agencies had identified key ICT assets that are vital for service delivery

4.1 Eight out of nine agencies identified the assets they consider essential for service delivery. The level of sophistication used to record and monitor key ICT assets varied across agencies. Some agencies had ICT asset registers, and some had asset management plans in place, although many of these were outdated.

4.2 Registers, where they existed, could be significantly enhanced through regular review and a consistent preparation format across agencies. Ownership of the key asset and its upkeep and/or replacement was not always distinguishable.

4.3 Agencies were largely managing key ICT assets effectively, but not necessarily efficiently.

4.4 In some cases, it was difficult for agencies to identify essential ICT assets or to fully understand the consequences of the development/replacement of them. For

example, four agencies advised the traceability and monitoring of critical ICT assets can be difficult following the implementation of machinery of government changes. Another example is decentralisation of critical ICT asset management where different parts of an agency manage their own ICT assets. Finally, where there is cross-agency reliance or sharing of systems it is difficult for ICT functions within agencies to have a complete or clear view of critical ICT assets. For example:

- one agency often provided common platform/support to other agencies but it was not always clear whether these services were within the standard agency remit or an additional or project offering
- two agencies provided support to various government entities
- there was a shared service arrangement between two agencies
- all agencies contained examples of decentralised ICT asset management.

4.5 In the cross-agency examples, well defined SLAs would assist in enhancing visibility of reliance on ICT systems or services, and could avoid agencies unintentionally adversely impacting another agency's ability to provide essential services. In terms of current usage of SLAs, we were only able to sight one and it was in draft form.

Long-term or high value key ICT asset replacement requires significant progression in departmental planning to identify traditional or alternative replacement service delivery models

4.6 A critical element in the consideration of replacement or renewal of key ICT assets are the risks associated with that ICT asset. Risks such as those related to maintaining and supporting the asset, risks associated with the likelihood the asset may cease to be effective or become outdated, or any other significant risk that may lead to a compromised ability for the agency to deliver essential services should be central to the planning and prioritisation for replacement.

4.7 The level of rigour and maturity applied to various aspects of planning varied across agencies and this was also the case for risks associated with asset replacement.

4.8 Seven agencies assessed risks associated with key ICT assets at a high level. Generally, short, medium and long-term planning for key ICT assets was included within the ICT Strategic Plans. However, long-term or high value key ICT asset replacement requires significant progression in departmental planning to identify traditional or alternative service delivery models. Some considerations could include:

- service delivery options
  - common versus unique agency opportunities
  - future proofing/citizen service delivery expectations
- pay for service models

4.9 A progression in planning maturity would draw out key risks, and contingency plans for the replacement, upgrade or renewal of these assets. This internal effort is required prior to undertaking any funding requests.

4.10 In cases where the management of critical ICT assets was spread across business units within an agency, the central ICT function did not always have visibility on key ICT asset management, including risk identification, because ownership sat within the business function. There appeared to be limited mechanisms in place to collaborate on or respond to the management risks associated with these ICT assets.

4.11 Risks associated with not achieving desired investment outcomes, due to lack of funding or otherwise, and resultant contingency plans were not well documented. Key actions could include:

- determining an ICT risk appetite which should be based on the agencies overall risk appetite
- utilising ICT risk registers
- including individual risk assessments for critical assets
- better monitoring and centralised reporting of critical asset risks across agencies with decentralised management of ICT assets
- better assessment of contingency plans (including alternative funding considerations) for critical ICT assets
- utilising SLAs for agencies with reliance on other agencies critical assets.

4.12 Agencies had prepared business cases and funding applications for critical ICT asset replacement without sufficient insight into decision-making protocols. Some agencies expressed frustration of having little influence over funding outcomes.

4.13 Business cases and funding applications showed a lack of contingency planning and a number of instances of the 'do nothing' option for extremely aged infrastructure. For example, one project that participated in the SIIRP did not receive funding following an unsuccessful Budget submission and no contingency plan was prepared for this event. The lack of funding left this agency half way into a large transformation project, maintaining new and legacy systems. Rather than the expected project efficiency gains being delivered, this had a significant and ongoing effect on the IT department, which had already been liquidating assets to fund ICT projects.

4.14 In assessing whether key ICT assets were identified within ICT planning on a risk basis, or contingency basis for replacement, upgrade or renewal, we identified significant room for improvement across most agencies for long-term or high value ICT asset replacement.

Funding for short-term replacement or renewal was considered but longer term funding for significant key ICT asset replacement or renewal projects was difficult to plan for and obtain

4.15 Agencies are responsible for scoping projects, allocating appropriate resourcing and obtaining funding.

4.16 Where it existed, evidence showed planning over the short term only, usually up to 12 months. There was a consistent lack of long-term planning to anticipate key system replacement and IT transformation. Agencies commented that in some cases larger spending requirements were put off or simply not planned because it was seen as 'pointless' due to a perceived lack of appetite for the government to fund large scale ICT asset replacements. This resulted in a number agencies retaining aged ICT infrastructure, some of which were no longer supported by the vendor.

4.17 Planning for long-term ICT infrastructure replacement was difficult for agencies. Not only do they need an understanding of the current state of their ICT environments and their desired target state, they also need to understand where they rank in the list of WoG investment priorities. Without a WoG ICT vision founded on information across all agencies, this clarity around investment prioritisation is not available. This lack of understanding and insufficient planning has resulted in:

- agencies undertaking work required without planning the associated internal costs
- underestimation of the internal resourcing cost required for the implementation of replacement ICT assets
- agencies taking on board projects in a reactive manner without a current ICT Strategic Plan
- significantly aged infrastructure remaining operational. This audit identified key ICT assets up to 37 years old
- critical support, security, integration, reporting and procedural functions that aged systems cannot support, together with a dwindling resource of support staff or services to maintain these systems
- management and/or replacement of aged ICT assets becoming prohibitive to agencies
- no cross-agency planning and associated investment proposals.

4.18 While some agencies attempted to self-fund their ICT investment through sale or lease of assets, reallocation of internal funding or by obtaining Australian Government funding, agencies were generally reliant on funding obtained through successful Budget submissions for ICT investment. This made longer term funding for significant ICT replacement or renewal, or transformational projects, difficult to plan for.

4.19 There appeared to be multiple channels for agencies to outline consequences of not having a project funded, or the potential impact of an essential ICT asset failing. This included the Budget submission process, the governance framework where DSB, DSDSC and DSAG provide advice to DPAC on ICT investment to the Budget Committee[19] and communication with respective Ministers. However, for long-term or large scale ICT asset funding there was no observable WoG planning and prioritisation framework based on information sourced through any of the above channels.

4.20 The risk of key ICT asset failure potentially exposes the government to an inability to provide essential services, inaccuracy or loss of data, poor planning decisions and security vulnerability.

4.21 Long-term planning for key ICT asset replacement is ineffective. As a result, there is potential for key ICT asset failing, leading to an inability to deliver essential services. This issue will be further compounded as time progresses and legacy systems that are not replaced or upgraded become more obsolete.

[19] A standing committee of the Tasmanian Cabinet whose role includes consider and deliberating on Budget submissions provided by agencies and other agencies

5. Has the government facilitated an investment evaluation and prioritisation approach to ICT investment that is effective?

In this chapter we assessed if the government facilitated an effective investment evaluation and prioritisation approach to ICT investment to support and deliver efficient and effective government services that meet the needs and expectations of the government and the Tasmanian community. This included assessing whether:

- ICT investment was prioritised from a WoG perspective
- agency approaches to securing ICT investment funding were efficient and effective.

Chapter summary

The government had not set an ICT vision across WoG. 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 that can be measured.

There was no strategic approach to prioritising agency ICT investment proposals that could better inform and guide government and Budget decision making in this crucial area from a WoG benefit context or an agency specific context. While recognising that ICT project Budget submissions are ultimately considered in the context of the full range of the government's policy priorities and the Budget position, insight into the prioritisation of ICT investment from a WoG perspective would assist the Budget process. The DSB had a key role to play in informing investment decisions. As the key body in the governance framework, one of its key responsibilities was to agree strategic and investment priorities to support and deliver efficient and effective government services that meet the needs and expectations of the government and the Tasmanian community.

Agencies were generally reliant on funding obtained through successful Budget submissions for ICT investment and they were responsible for effectively presenting their case for the provision of funding. Agencies had the option to submit proposed ICT projects through the SIIRP but many agencies perceived the SIIRP as onerous given the uncertainty of success in securing Budget funding.

Agencies rarely collaborated on SIIRP submissions and also perceive limited feedback was received when there is an unsuccessful Budget submission. Feedback on unsuccessful SIIRP submissions would provide insights that would lead to higher quality SIIRP submissions in the future.

The lack of a WoG ICT vision adversely impacts the prioritisation of ICT investment

5.1 The government had not set an ICT vision across WoG. 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 that can be measured. Without a WoG ICT vision various underlying aspects of broader ICT planning and execution cannot be effectively delivered. Definition of short, medium and long-term goals and the delivery mechanism would allow agencies to focus on their core services.

5.2 While recognising that ICT project Budget submissions are ultimately considered in the context of the full range of the government's policy priorities and the Budget position, insight into the prioritisation of ICT investment from a WoG perspective would assist the Budget process.

5.3 DSB, DSDSC and DSAG have an important role in providing advice to DPAC on ICT investment. DPAC, in turn, provides advice to the Minister and Budget Committee.

5.4 DSB has a key role to play in informing investment decisions. As the key body in the Digital and ICT governance and decision making framework, one of its key responsibilities is to agree strategic and investment priorities to support and deliver efficient and effective government services that meet the needs and expectations of the government and the Tasmanian community. The lack of a WoG ICT vision inhibited the DSB's ability to develop a strategic approach to support prioritising agency ICT investment proposals that could better inform and guide government and Budget decision making in this crucial area.

5.5 An assessment framework that ensures ICT investment is prioritised across WoG according to comprehensive evaluation criteria would inform the government as to where investment funding is needed most. Examples of WoG ICT project evaluation and investment criteria are:

- alignment to government strategy and strategic importance
- ability to mitigate significant risks
- criticality/urgency of replacement or renewal
- ability to comply with WoG ICT policies and standards
- service orientation, including 'as a service' sourcing models
- provision of online access and ability to support the sharing of data, as appropriate
- ICT projects that provide WoG benefits, such as leverage across a number of agencies, opportunities for collaboration and ICT solution re-use
- standardisation and interoperability of technologies and solutions
- value to government and citizens over the life of the investment.

5.6 While, at an agency level, much of the above may be included in a well-developed SIIRP investment proposal or Budget submission we note this was not undertaken at a broader informed WoG level. In the absence such WoG prioritisation, agency key ICT assets and systems may be expected to remain operational well past their intended useful life, exposing agencies to significant service delivery interruption should they fail.

Agencies perceived participation in the SIIRP as onerous given the uncertainty of success in obtaining Budget funding

5.7 As noted in Chapter 4, agencies were generally reliant on funding obtained through successful Budget submissions for ICT investment. Budget submissions and project business cases are important conduits through which information is provided to enable the assessment of requests for Budget funding. The information provided within these documents should effectively argue the case for the allocation of funding including highlighting the need for ICT renewal and replacement.

5.8 To assist with the evaluation of General Government Sector infrastructure investment proposals, including ICT investment proposals, Treasury established the SIIRP. However, not all infrastructure projects have to go through the SIIRP in order to receive funding, and a project meeting the requirements of the SIIRP is not guaranteed an allocation of Budget funding for the project. As part of the SIIRP, agencies have the opportunity to seek funding to help meet the requirements of the SIIRP. For example, funding can be sought to facilitate the preparation of a detailed business case for a project or to engage consultants to undertake planning or a specific aspects of early project stages.

5.9 The objective of the SIIRP is to ensure proposed infrastructure projects:

- appropriately meet the needs of the community
- provide clear and strong links to specific government policy priorities and the government's strategic direction
- demonstrate strong evidence of prioritisation within the context of an agency's competing priorities, requirements and its capacity to deliver
- demonstrate direct links with specific agency asset management strategies, including objectives outlined in strategic asset management plans
- have been appropriately scoped and planned
- are based on reliable and realistic cost estimates
- are able to be delivered by agencies in accordance with the specified timeframes and within the project budget allocations.[20]

[20] Source: Structured Infrastructure Investment Review Process (SIIRP), Point 1 Guidelines (October 2015)

5.10 A comprehensive SIIRP template is available for agencies to use in preparing submissions. The template requires project information, project justification, risk and dependencies (including external conditions and critical success factors) and a project optional analysis. Agencies advised a submission prepared using the template requires a considerable investment of time and resources.

5.11 The perception of the SIIRP process varied. One agency had never been involved and had very limited understanding of the process. Another agency indicated the SIIRP was similar to an internal Budget submission and presented limited value compared to that process. Agencies used both processes in preparing investment proposals.

5.12 The SIIRP can provide important feedback to agencies on the strength of their investment proposals and potentially enhance the likelihood of the project receiving Budget funding. While the Treasury indicated the SIIRP process to be an effective process to evaluate investment proposals, many agencies perceived the SIIRP as onerous given the uncertainty of success in securing Budget funding.

Agencies rarely collaborate on SIIRP submissions and limited feedback is received when unsuccessful

5.13 Where mutually beneficial agencies should collaborate to plan inter-agency projects and request joint funding.

5.14 In one instance, a SIIRP submission was reliant on another agencies successful SIIRP submission to provide the required data sets for their investment plans. Only one of the submissions was successful in securing Budget funding. This left the successful agency with an inability to obtain required datasets for their approved SIIRP investment. The resulting impact has the potential of an unsuccessful investment outcome, which was the case in this instance as the agency with the unsuccessful SIIRP and Budget submission was left with a partially installed platform.

5.15 Feedback is provided from Treasury in relation to SIIRP submissions at different points in the process. However, agencies did not always receive written feedback on unsuccessful SIIRP submissions. While it is the government's decision on what to fund, feedback on submissions would provide insights that would lead to higher quality SIIRP submissions in the future.

6. Do the government and agencies have plans to provide a pathway to digital capabilities?

In this Chapter we assessed if there were plans for government and agencies individually that identified emerging needs and possible future service delivery mechanisms.

Chapter summary

Digital capability across the government and agencies, including future delivery models, and potential efficiencies to be gained through shared services or business processing, were in the early stages of development. The recent release of *Our Digital Future* provided high level direction for digital transformation across WoG and individual agencies.

Digital capability across the government and agencies, including future delivery models, and potential efficiencies to be gained through shared services or business processing, are in the early stages of development

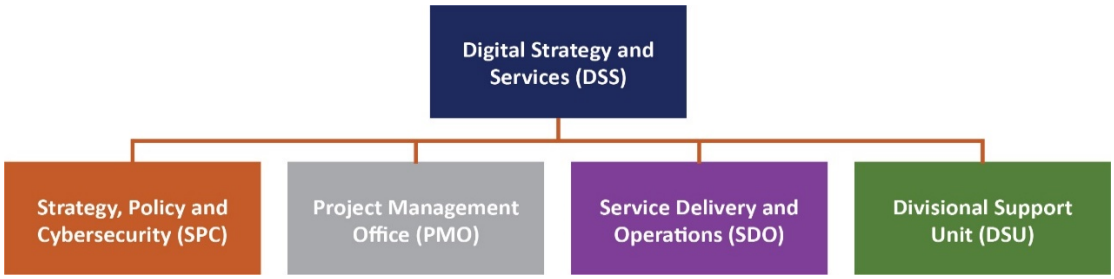
5.16 Some agencies had created digital strategies and were more advanced than others. Prior to the release of *Our Digital Future* , initiatives driven by government have been focussed on policy such as Open Data (Jan 2016), cybersecurity, the cloud , and the consolidation of shared infrastructure and WoG single contract projects such as Office 365.

5.17 The government was transitioning toward a more strategic focus to enable DSS to anticipate and build coherence and value for the agencies through digitalisation of government service offerings.

5.18 DSS released two key documents: *Digital Foundations, meeting the government service expectations of all Tasmanians*, a program business case (January 2019) and *DSS 2021, a two-year strategic plan for Digital Strategy and Services (Draft)* (DSS 2021).

5.19 DSS 2021's purpose is to advise and support government and its agencies to achieve priority objectives and core business outcomes through the provision of fit-for-purpose digital policy and technology solutions. It contained ten key priorities including a focus on whole-of-government benefits, a more proactive decision making process, and forming strategic relationships all of which demonstrate consideration of a coordinated and considered approach across the government. It also outlined an aspirational DSS organisational structure as shown in Figure 6 below.

Figure 6: DSS organisational framework



Source: DSS 2021 "A two-year strategic plan for Digital Strategy and Services" (Draft)

However, the proposed DSS framework is unfunded and at the time of the audit DSS lacked a formal mandate to empower it to act across the agencies.

5.20 The draft DSS 2021 did not identify measurable goals to monitor the success or progress of DSS, although it does outline criteria to develop a baseline to measure DSS' performance against.

The release *Our Digital Future* provides high level direction for digital transformation for the government and agencies

5.21 *Our Digital Future* represents another step towards progressing digital capability across the government. However, with the status of the documented major actions, it acknowledges it is in the early stages of development and a lot of work remains to be done.

5.22 Funding of the initiatives is not specified at either the WoG or agency level and its success will be impacted on the ability to secure adequate funding for its implementation.

Acronyms and abbreviations

CIO	Chief Information Officer
DPAC	Department of Premier and Cabinet
DSAG	Digital Services Advisory Group
DSS	Digital Strategy and Services
DSB	Digital Services Board
DSDSC	Deputy Secretaries Digital Services Committee
ICT	Information and Communications Technology
IT	Information Technology
KPI	Key Performance Indicator
SIIRP	Structured Infrastructure Investment Review Process
TAO	Tasmanian Audit Office
Treasury	Department of Treasury and Finance
WoG	Whole of government

Audit Mandate and Standards Applied

Mandate

Section 23 of the *Audit Act 2008* states that:

(1) The Auditor-General may at any time carry out an examination or investigation for one or more of the following purposes:

- (a) examining the accounting and financial management information systems of the Treasurer, a State entity or a subsidiary of a State entity to determine their effectiveness in achieving or monitoring program results;
- (b) investigating any mater relating to the accounts of the Treasurer, a State entity or a subsidiary of a State entity;
- (c) investigating any mater relating to public money or other money, or to public property or other property;
- (d) examining the compliance of a State entity or a subsidiary of a State entity with written laws or its own internal policies;
- (e) examining the efficiency, effectiveness and economy of a State entity, a number of State entities, a part of a State entity or a subsidiary of a State entity;
- (f) examining the efficiency, effectiveness and economy with which a related entity of a State entity performs functions –
  - (i) on behalf of the State entity; or
  - (ii) in partnership or jointly with the State entity; or
  - (iii) as the delegate or agent of the State entity;
- (g) examining the performance and exercise of the Employer's functions and powers under the *State Service Act 2000*.

(2) Any examination or investigation carried out by the Auditor-General under subsection (1) is to be carried out in accordance with the powers of this Act

Standards Applied

Section 31 specifies that:

> 'The Auditor-General is to perform the audits required by this or any other Act in such a manner as the Auditor-General thinks fit having regard to -
>
> (a) the character and effectiveness of the internal control and internal audit of the relevant State entity or audited subsidiary of a State entity; and
>
> (b) the Australian Auditing and Assurance Standards.'

The auditing standards referred to are Australian Auditing Standards as issued by the Australian Auditing and Assurance Standards Board.

Phone (03) 6173 0900
Fax (03) 6173 0999
Email admin@audit.tas.gov.au

Address Level 8, 144 Macquarie Street
Hobart, 7000
Postal GPO Box 851, Hobart 7001

Launceston Office

Phone (03) 6173 0971
Web www.audit.tas.gov.au

Address 4th Floor, Henty House
1 Civic Square, Launceston