Tasmanian
Audit Office

Report of the Auditor-General No. 8 of 2017-18

Follow up of selected Auditor-General reports: March 2015 to May 2015

May 2018

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).*

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 issue a variety of reports to State entities and we report periodically to the 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.

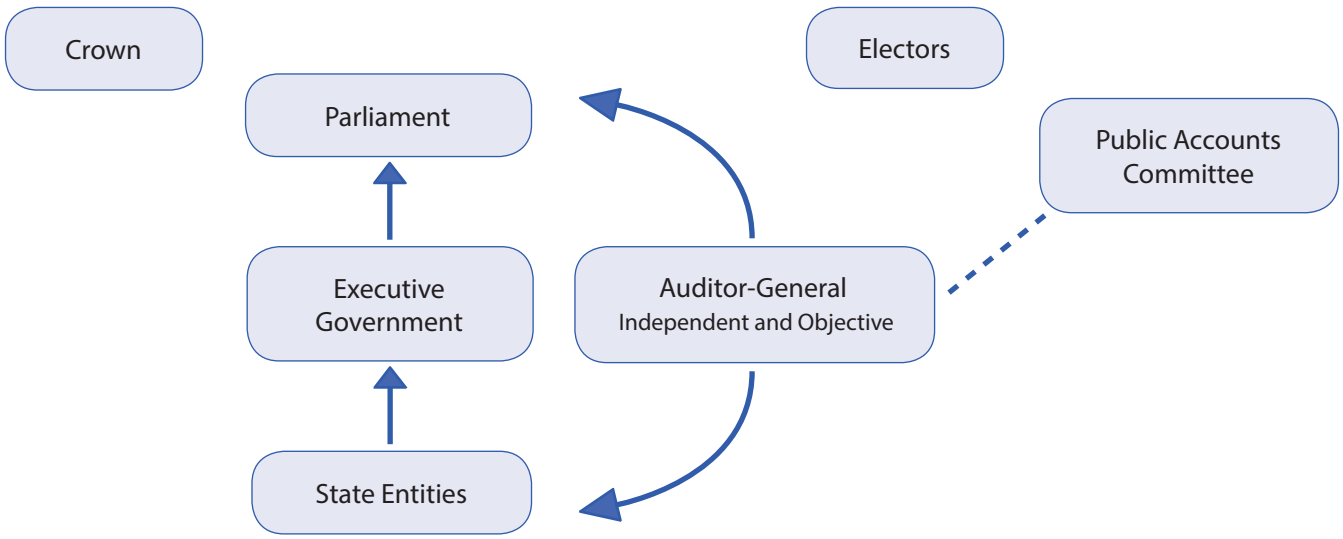
We can also carry out investigations but only relating to public money or to public property. In addition, the Auditor-General is now responsible for state service employer investigations.

Performance and compliance audits are reported separately and at different times of the year, whereas outcomes from financial statement audits are included in one of the regular volumes of the Auditor-General's reports to the Parliament normally tabled in May and November each year.

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

The Auditor-General's role as Parliament's auditor is unique.



2018
PARLIAMENT OF TASMANIA

Report of the Auditor-General
No. 8 of 2017-18

Follow up of selected Auditor-General reports: March 2015 to May 2015

May 2018

Presented to both Houses of Parliament in accordance with the requirements of Section 30 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: 978-0-9954292-6-0

This report is printed on FSC Mix Paper from responsible sources.

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

24 May 2018

President
Legislative Council
HOBART

Speaker
House of Assembly
HOBART

Dear President

Dear Speaker

Report of the Auditor-General No. 8 of 2017–18: Follow up of selected Auditor-General reports: March 2015 to May 2015

This report has been prepared consequent to examinations conducted under section 23 of the *Audit Act 2008*. The objective of the audit was to form conclusions on the extent to which recommendations made in the four selected reports have been implemented and the appropriateness of the rationale or evidence to support non-implementation.

Yours sincerely

Ric De Santi
Acting Auditor-General

Page left blank intentionally

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

FOREWORD

The Office's purpose is to provide independent assurance to the Parliament, our primary client, and the community on the performance and accountability of the Tasmanian public sector. One way in which this is done is to conduct performance and compliance audits, an objective of which is the identification of areas for potential improvement. These audits resulted in reports containing recommendations which were, at the time of reporting, generally supported by the State entities who were the subjects of our work.

Importantly, neither I nor the Office, has executive authority and State entities are not compelled to implement recommendations made. However, it is our expectation that recommendations will be either adopted or at least seriously considered by State entities.

Follow-up audits are carried out to inform Parliament on the extent to which the recommendations from previous audits have been implemented and the appropriateness of the rationale or evidence to support non-implementation.

This follow-up audit provides Parliament with information about the extent to which State entities have acted on recommendations made in four reports tabled between March and May 2015.

Ric De Santi

Acting Auditor-General

24 May 2018

AUDITOR-GENERAL'S 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 on the follow-up of the implementation of recommendations made in four previous performance audits. This audit was completed to provide Parliament with information about the extent to which State entities have acted on recommendations made in four reports tabled between March and May 2015:

- Report of the Auditor-General No. 8 of 2014–15 *Security of information and communications technology (ICT) infrastructure*
- Report of the Auditor-General No. 9 of 2014–15 *Tasmanian Museum and Art Gallery: compliance with the* National Standards for Australian Museums and Galleries
- Report of the Auditor-General No. 10 of 2014–15 *Number of public primary schools*
- Report of the Auditor-General No. 11 of 2014–15 *Road management in local government*.

AUDIT OBJECTIVE

The objective of the audit was to form conclusions on the:

- extent to which recommendations made in the reports have been implemented
- appropriateness of the rationale or evidence to support non-implementation.

AUDIT SCOPE

This Report covers four audits tabled between March and May 2015:

State entities involved	Recommendations
Security of information and communications technology (ICT) infrastructure Tabled 26 March 2015	
• Department of Treasury and Finance (Treasury) • Department of Primary Industries, Parks, Water and the Environment (DPIPWE) • Department of Premier and Cabinet (DPAC) • Department of Health and Human Services (DHHS) • Department of Police, Fire and Emergency Management (DPFEM), previously Police and Emergency Management (DPEM)	The report contained 44 recommendations. DPIPWE, DPAC, DHHS and DPFEM in general, accepted the recommendations. Treasury noted the recommendations.
Tasmanian Museum and Art Gallery: compliance with the National Standards for Australian Museums and Galleries Tabled 26 March 2015	
• Department of State Growth (State Growth) • Tasmanian Museum and Art Gallery (TMAG)	The report contained 11 recommendations. State Growth noted that the national standards were a set of ideals and the government intended to review the governance arrangements at TMAG. TMAG noted the recommendations and stated it would take them into consideration.

State entities involved	Recommendations
Number of public primary schools Tabled 26 May 2015	
• Department of Education (DoE)	The report contained seven recommendations. DoE agreed to take the recommendations into consideration.
Road management in local government Tabled on 26 May 2015	
• Central Highlands Council (CHC) • Devonport City Council (DCC) • Northern Midlands Council (NMC) • Waratah-Wynyard Council (WWC)	The report contained 15 recommendations. CHC, NMC and WWC accepted the recommendations. DCC noted the recommendations with some concerns regarding the audit methodology.

AUDIT APPROACH

The audit was conducted in accordance with the 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 approach included:

- requesting entities subject to the audits to self-assess the degree to which they had implemented the recommendations
- testing the assertions made by the entities as to the extent of implementation of the recommendations
- undertaking additional testing and revisiting the original audit tests where relevant
- undertaking discussions with respondent staff.

AUDIT COST

The audit cost $98 683.

MANAGEMENT RESPONSIBILITY

The entities had responsibility for acting on the recommendations contained in the original reports.

AUDITOR-GENERAL'S RESPONSIBILITY

In the context of this audit, my responsibility is to express a reasonable assurance conclusion on the extent to which the recommendations from the relevant previous audits have been implemented and the appropriateness of the rationale or evidence to support non-implementation.

SUBMISSIONS AND COMMENTS RECEIVED

In accordance with section 30(2) of the *Audit Act* 2008, a summary of findings was provided to the Secretary of the relevant entity and other persons who, in the opinion of the Auditor-General, had a special interest in the report, with a request for submissions or comments. Responses, or a fair summary of them, are included in the Detailed Findings section of this Report.

AUDITOR-GENERAL'S CONCLUSION

Security of information and communications technology (ICT) infrastructure

ICT security is a critical risk, the impacts of which have been played out regularly in the media. We expect State entities to place a high priority on addressing this risk and leading the way in the implementation of risk mitigation strategies.

ICT security measures should ensure that all systems are secure and provide a safe environment for government:

- staff to carry out the entity's business
- customers to interact with the entity.

Treasury and DPAC substantially implemented our recommendations and DPFEM is progressing well. DPIPWE and DHHS have yet to fully address ICT security risk.

Recommendation

All entities continually assess the adequacy of their ICT security and ensure resources are allocated to address high risk areas.

Tasmanian Museum and Art Gallery: compliance with the *National Standards for Australian Museums and Galleries*

We are pleased to confirm that:

- State Growth has fully implemented the recommendations
- TMAG has fully implemented eight recommendations and has made significant progress on implementing the remaining recommendation.

Number of public primary schools

In recognition of the current government policy of no forced school closures, we accept the position taken by DoE in not implementing most of the recommendations in our 2015 report.

Road management in local government

We are pleased to confirm that CHC, DCC and NMC have either fully implemented or substantially implemented our recommendations.

WWC has fully or partially implemented the recommendations with the exception of two which it has delayed. These do not create a serious risk.

Ric De Santi

Acting Auditor-General

24 May 2018

DETAILED FINDINGS

1. SECURITY OF INFORMATION AND COMMUNICATIONS TECHNOLOGY INFRASTRUCTURE

1.1 Background

State entities rely heavily on information and communications technology (ICT) which supports key systems such as patient management, police operations and motor registry. Given the nature of information held within ICT systems, ICT infrastructure and data needs protection from equipment failure, data loss, misuse or cyber-attack[1].

Our audit in March 2015 involved a review of ICT physical infrastructure, applications and information security. Key elements of the audit incorporated prioritised strategies for cyber security listed by the Australian Signals Directorate (ASD)[2]. At least 85% of cyber intrusions responded to by ASD in 2011 involved unsophisticated techniques that would have been mitigated by the 'Top 4' mitigation strategies of:

- Whitelisting applications
- Patching applications
- Operating system patchings
- Minimising administrative privileges.

At the time of the 2015 audit, a whole-of-government project sponsored by DPAC was underway to produce an ICT Security Framework for application across all State entities. The project's terms of reference included producing a Government ICT Security Manual. At the time of our original audit, the work was not sufficiently advanced to be considered and our testing was done at an individual entity level.

The objective of the audit was to assess the effectiveness of security measures for ICT infrastructure in state entities. The scope of the audit included ICT physical infrastructure, applications and information. State entities subject to the audit were:

- Treasury
- DPIPWE
- DHHS
- DPAC
- DPEM, now DPFEM.

1.2 Conclusions from the 2015 audit

The main findings of the 2015 audit were that:

- Generally, the entities had reasonable security over most of their facilities, infrastructure and servers. However, there were some areas of inadequate security in most entities. Common problems included lack of policy on physical security, server room security and limited closed-circuit television (CCTV) coverage.
- Information was generally safe and secure with reasonable backup and access restrictions. However, all entities were at excessive risk from cyber-attack because of a lack of ASD-recommended mitigation strategies. Two other common areas of weakness were lack of testing of back-ups and access permissions.
- There was a widespread failure for entities to take a strategic approach to ICT security. This was evidenced by the lack of ICT security plans, incident recording systems, business continuity plans and disaster recovery plans.

1. Cyber-attack is a malicious attempt to damage, disrupt or gain access to a computer or a computer network. It can be particularly troublesome in terms of repair time, loss of data and breach of confidentiality.
2. Australian Signals Directorate (ASD), *Strategies to Mitigate Targeted Cyber Intrusions*, October 2012.

1.3 Recent developments

Since our 2015 audit, the Top 4 mitigation strategies have been expanded to become the 'Essential 8', which in addition to the original four noted previously, now also include:

- configure Microsoft Office macro settings
- user application hardening
- multi-factor authentication
- daily backup.

For the purpose of this audit, we re-assessed entities against the original Top 4 in place in 2015.

Since our 2015 audit, there has also been a move away from a compliance testing approach towards a more risk-based approach to protecting information and systems.

A whole-of-government approach has been taken with the establishment of the Office of eGovernment (eGovernment) in DPAC a number of years ago, which has focussed its efforts on developing templates and policies with the appointment of a Chief Information Officer in September 2017. eGovernment's purpose is to ensure the effective use, investment and governance of ICT across government and is responsible for:

- leading the development of an ICT strategy for government
- developing policies, standards and guidelines
- supporting key ICT projects across government
- supporting the governance of ICT
- building government statistical assets and capability.

eGovernment is currently developing a number of policies including:

- Tasmanian Government Cybersecurity Policy
- Tasmanian Government Cybersecurity Incident Response Plan
- Tasmanian Government Cybersecurity Incident Response Operational Roles and Responsibilities
- Cybersecurity Policy Responsibility Guide.

eGovernment is also developing a whole-of-government Information Classification Policy together with a number of agency policy templates and policies for vendors and third parties.

While eGovernment is responsible for developing policies at the whole-of-government level, departments remain responsible for developing their own policies and procedures that are more granular and applicable to their individual and often unique ICT environments.

eGovernment is not included in the scope of this audit but provides necessary context to the topic of ICT security.

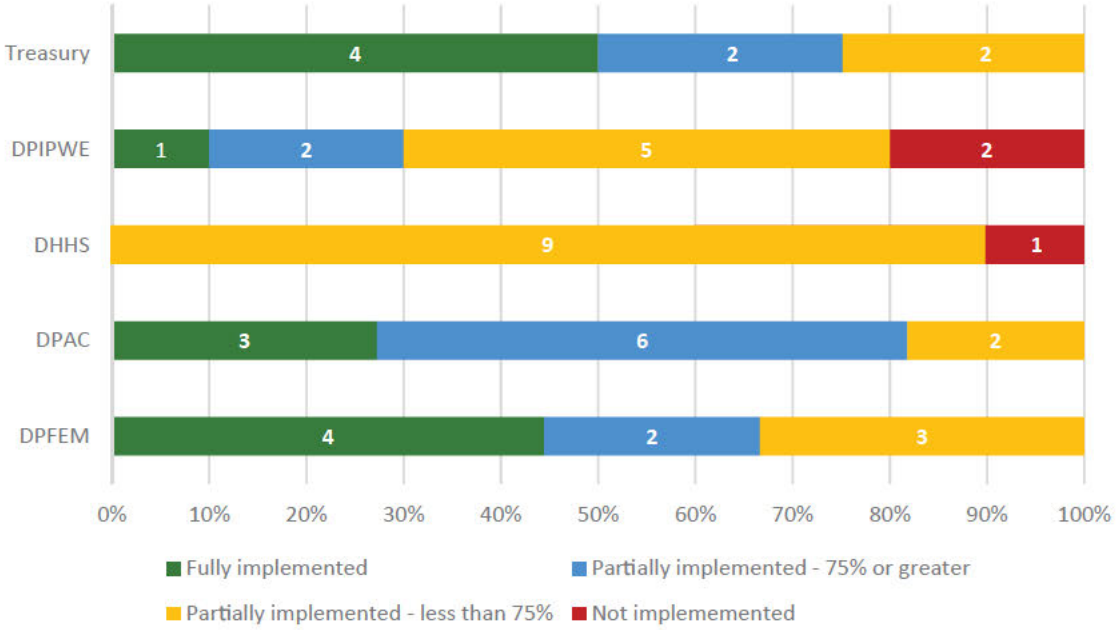
Most entities, including those covered by this audit, are now moving towards third-party hosting and service provision. In our opinion, notwithstanding the shift to external service provision and the work being undertaken by eGovernment, it remains essential to ICT security for any government agency to demonstrate:

- risk management — adopting a risk-based approach to identify and assess the impact of threats affecting critical ICT services
- high resilience — ensuring that critical business and ICT services are robustly designed, implemented and maintained to minimise occurrences of disruption to the entity's business services and operations
- rapid recovery — establishing business and ICT continuity and disaster recovery plans and priorities to enable timely resumption of critical ICT services in the event of disruptions
- ongoing preparedness — continual improvement through periodic reviews of plans, exercises and audit compliance.

1.4 Status of recommendations

The 2015 audit resulted in 44 recommendations. As one recommendation applied to all five entities, a total of 48 recommendations were assessed. Figure 1 shows our assessment of the extent to which the recommendations have been implemented.

Figure 1: Extent of recommendation implementation



The implementation status of the recommendations is summarised in Table 1 below.

Table 1: Security of ICT infrastructure — status of implementation of recommendations

No.[a,b]	Recommendations (abbreviated)	Treasury	DPIPWE	DHHS	DPAC	DPFEM
5[c]	Fully implement at least the 'Top 4' mitigation strategies from Strategies to Mitigate Targeted Cyber Intrusion	P 75%	P 50%	P 10%	P 50%	P 90%
1	• Include physical security of servers and server rooms in ICT security policy • Use CCTV monitoring	✓				
3 21 30	Test backups at a frequency commensurate with risk	✓		P 25%	✓	
4 31 39	Disable local administrator accounts	✓			P 50%	P 50%
6	• Review monitoring of system access by business units • Audit access to ensure consistency across all systems	P 50%				
7 15 24 33 41	Develop a specific ICT security plan and update ICT security risk review	✓	✗	P 5%	P 75%	✓

No.[a,b]	Recommendations (abbreviated)	Treasury	DPIPWE	DHHS	DPAC	DPFEM
8 25	Make greater use of inbuilt IT controls such as enforcing password standards and controls over the use of unauthorised media	**P** 75%		**P** 10%		
16 42	Implement inbuilt IT controls over the use of unauthorised media		✗			**P** 50%
9	Conduct a full disaster recovery test	**P** 50%				
10 19	• Update ICT security policy • Upgrade access controls, alarms and hazard protection at specific server rooms where necessary		**P** 75%	**P** 33%		
11	• Provide protective covering for any exposed building cabling • Provide basic security of switches and routers		**P** 50%			
12	• Use off-site storage for all back-up tapes • Record back-up procedures • Maintain test logs		**P** 80%			
13	• Consider the use of firewalls for workstations • Disable local administrator accounts		**P** 50%			
14	• Develop a policy to ensure that access to confidential information is valid and that no unused accounts exist • Implement regular testing • Monitor user access		**P** 50%			
17 26 43	Implement an ICT security incident recording and management system		✓	**P** 5%		✓
18 27 44	• Develop business continuity plans • Develop ICT security disaster recovery plans • Test plans regularly		**P** 20%	**P** 10%		**P** 75%
20 29 37	• Set standards for physical security • Implement specific protections accordingly			✗	**P** 75%	**P** 50%
22	• Implement application-based workstation firewalls • Implement multi-factor authentication for external access • Address consultant's concern regarding poor network segmentation			**P** 30%		

No.[a,b]	Recommendations (abbreviated)	Treasury	DPIPWE	DHHS	DPAC	DPFEM
23	• Develop a policy to ensure that access to confidential information is valid and that no unused accounts exist that can be wrongfully used • Audit access privileges to bring accounts up to date • Implement regular testing and monitoring of user access			**P** 10%		
2	• Outline requirements for varying levels of security • Develop guidelines to allow departments to self-assess and accredit departments' various security zones				**P** 75%	
28	• Upgrade coverage of physical security in ICT security policy • Review construction of server rooms • Review expanded use of CCTV • Implement greater hazard protection				**P** 80%	
32	Enforce password parameters in line with departmental policy				✓	
34	Make greater use of in-built IT features such as: • time-outs on personal computers • enforced password standards • controls over unauthorised media and software				**P** 75%	
35	Modify help-desk systems to enable the recording of security near misses				✓	
36	Improve disaster recovery plans by: • identifying responsible officers • linking to risk management documentation • covering security breaches and cyber-attacks • setting recovery time objectives • further documenting tests				**P** 75%	
38	Document backup and restore procedures					✓
40	• Fully document access procedures • Implement a regular program of access testing					✓
	Number of recommendations	**8**	**10**	**10**	**11**	**9**

✓ Fully implemented, × Not implemented, **P** Partially implemented (%), Blue shading - not applicable.

Notes: *(a) Multiple recommendation numbers in each row arise where the same recommendation has been made separately for each entity in the original report*

(b) Recomendation number in original report

(c) Single recommendation applying to all entities.

1.4.1 Department of Treasury and Finance

Eight recommendations related to Treasury.

Treasury fully implemented four recommendations:

- ICT security policy covers physical security of servers and server rooms and CCTV is used to monitor server rooms (Recommendation 1).
- Test backups at a frequency commensurate with risk (Recommendation 3).
- Disable local administrator accounts (Recommendation 4).

  While not strictly complying, we were persuaded that some IT technical issues required the retention of local administrator accounts. Treasury uses an alternative password control solution to mitigate the risk, which we considered reasonable.
- Develop a specific ICT security plan and update ICT security risk review (Recommendation 7).

  This was reviewed by Treasury's Corporate Management Group in August 2017 and ICT security risks were reviewed by its Audit and Risk Management Committee in December 2015.

Treasury partially implemented four recommendations:

- Fully implement at least the 'Top 4' mitigation strategies from the ASD publication: *Strategies to Mitigate Targeted Cyber Intrusions* (Recommendation 5).

  Limited whitelisting is running on a small number of computers with full rollout expected by July 2018. Treasury advised that whitelisting will be achieved on all its devices with the installation of Windows 10.

  The other three strategies — patching applications, operating system patching and minimising administrative privileges — have been fully implemented.

  Treasury is taking sufficient action to address this recommendation.
- Review monitoring of system access by business units to ensure consistency across all systems (Recommendation 6).

  We noted that Treasury's ICT security policy assigns responsibility to business system owners for ensuring approved system access/revocation is appropriately applied, managed and regularly audited. While this is a responsibility of each business system owner across Treasury, the IT branch obtains confirmation from business system owners every six months on whether system access/revocation has been reviewed. We were unable to sight documentary evidence to confirm this.

  While Treasury is progressing this recommendation, the sufficiency of the documentary evidence could be improved.
- Greater use of inbuilt IT controls such as enforcing password standards and controls over the use of unauthorised media (Recommendation 8).

  Passwords met password standards with users unable to disable automatic timed lockouts but there was no control over unauthorised media[3]. Treasury advised the rollout of Windows 10 will address this issue with full rollout expected by July 2018.

  Treasury is on track to implement this recommendation if it maintains its implementation schedule.
- Conduct a full test of disaster recovery and business continuity plans (Recommendation 9).

  Treasury advised that, in the three years since our audit, its ICT infrastructure has changed dramatically and much of it has been outsourced with the following components no longer run by Treasury, but provided 'as a service':
    - servers (production and test)
    - network services (both wide area network and local area network)
    - desk phones and queues
    - web and proxy services

3. Unauthorised media is usually optical disks and USB memory that are introduced to a computer without permission

- email, instant messaging
- SharePoint web services
- SQL database management.

Because of this, a traditional full disaster recovery exercise focussing on server (host) level recovery (which was appropriate and required at the time of the 2015 audit), is no longer feasible. Instead, Treasury is focussed on end-to-end disaster recovery tests of different infrastructure and system components. These tests better simulate an actual disaster that is likely to be experienced with the outsourced services being used. Over the past year, Treasury has completed end-to-end disaster recovery testing of servers (using recovery options available from the provider) incorporating:

- budget system
- revenue system
- content management system
- SQL database systems.

Treasury advised that it will also be simulating a cybersecurity breach and running an end-to-end disaster recovery test on this scenario later in 2018.

Treasury is on track to implement this recommendation if it maintains the implementation schedule.

1.4.2 Department of Primary Industries, Parks, Water and the Environment

Ten recommendations related to DPIPWE.

DPIPWE fully implemented one recommendation being to introduce an ICT security incident recording and management system (Recommendation 17).

DPIPWE partially implemented seven recommendations:

- Fully implement at least the 'Top 4' mitigation strategies from the ASD publication: *Strategies to Mitigate Targeted Cyber Intrusions* (Recommendation 5).

  Application whitelisting is still being trialled after which it will be rolled out across the whole department. Some patching applications are still required to be manually implemented. However, operating system patching and minimising administrative privileges have been fully implemented.

  DPIPWE is taking sufficient action to address this recommendation. We note its rate of implementation is the same as DPAC (50%), less than Treasury (75%) and DPFEM (90%) but greater than DHHS (10%) .

- Update the ICT security policy and upgrades access controls, alarms and hazard protection at specific server rooms (Recommendation 10).

  One server room has been modified but another server room remains in the same condition as inspected in 2015. DPIPWE advised it will be moving out of the other server room to a secure third party data centre during 2018-19.

  DPIPWE (75%) has substantially implemented this recommendation. However, three years to either bring the second server room up to standard or to have relocated is considered a lengthy delay. DPIPWE's progress is greater than that of DHHS (33%).

- Provide protective covering for exposed building cabling and provide basic security of switches and routers (Recommendation 11).

  Switches and routers are password protected but some fibre optic cabling is still not adequately protected. We were advised that fibre-optic cabling is extremely difficult to compromise but nonetheless it is still possible to do so. Therefore we are not convinced that DPIPWE has taken sufficient action to implement this recommendation.

- Provide off-site storage for all backup tapes. Backup procedures should be recorded and testing logs maintained (Recommendation 12).

  Backup procedures are recorded and testing logs maintained. However, backup tapes Although two adjacent sites were merely exchanged rather than stored completely off-site.

Although DPIPWE had substantially implemented this recommendation, full implementation could have been achieved.

- Install firewalls to all workstations and disable local administrative accounts (Recommendation 13).

  Not all workstations have firewalls installed and not all local administrator accounts have been disabled. DPIPWE considers it inappropriate to disable local administrator accounts as it uses them to resolve issues when the network connection is not available on computer devices. DPIPWE's explanation appears reasonable as other entities have taken a similar course of action.

- Develop a policy to ensure access to confidential information is valid and ensure no unused accounts exist. Implement regular testing and monitoring of user access. (Recommendation 14).

  A policy is in place to regulate access to confidential information and was last reviewed in late 2017. The policy regarding no unused accounts exists but is not fully in place. DPIPWE produces a weekly active directory report that tests and monitors user access. This process is not fully documented, however, we sighted the report and noted that it is being acted upon.

  DPIPWE has acted on our recommendation but needs to finalise the policy on accounts that are no longer used and complete documenting the process.

- Develop business continuity plans and ICT security disaster recovery plans and test plans regularly (Recommendation 18).

  Business continuity and disaster recovery plans are not in place, although a draft copy of the business continuity plan was provided and DPIPWE is currently consulting with its business units to determine recovery priorities.

  DPIPWE could place greater priority on implementation of this recommendation as disaster recovery and business continuity plans are crucial documents for ensuring the continuity of the entity in the case of a significant event.

DPIPWE had not implemented two recommendations:

- Implement an ICT security plan and associated risk management plan (Recommendation 15).
- Implement inbuilt controls over the use of unauthorised media (Recommendation 16).

The reasons provided for non-implementation were:

- awaiting endorsement of a whole-of-government policy covering ICT security plans
- Windows 10 has not been fully rolled out with associated mitigating software to prevent unauthorised media penetration.

The reasons provided by DPIPWE are considered unsatisfactory as:

- Recommendation 15 had been fully implemented by Treasury and DPFEM, substantially implemented by DPAC (75%) and commenced by DHHS (25%)
- DPFEM (50%) is progressing Recommendation 16.

1.4.3 Department of Health and Human Services

Ten recommendations related to DHHS.

DHHS partially implemented nine recommendations:

- Fully implement at least the 'Top 4' mitigation strategies from the ASD publication: *Strategies to Mitigate Targeted Cyber Intrusions* (Recommendation 5).

  Windows 10 will be rolled out over the next two years, which will allow implementation of the mitigating strategies. Application whitelisting is in place for some workstations now running Windows 10. DHHS is recruiting to fill positions to enable better implementation of this recommendation.

  Compared to the other agencies, DHHS (10%) is behind in implementing this recommendation, with DPFEM (90%) and Treasury (75%) substantially implementing and DPIPWE (50%) and DPAC (50%) having progressed implementation.

- Upgrade access controls, alarms and hazard protection at specific server rooms (Recommendation 19).

  DHHS has six server sites around the State, including hospitals. Our inspection of the two non-hospital servers satisfied us that these sites have adequate access controls, alarms and hazard protection. However, the same level of protection does not exist at the hospital sites as DHHS is awaiting the completion of the whole-of-government standards for physical security before upgrading all server rooms.

  DHHS (33%) has not taken sufficient action to implement this recommendation when compared with DPIPWE (75%) who has substantially progressed implementation.

- Test backups at a frequency commensurate with risk (Recommendation 21).

  DHHS carries out regular automatic backups and restore system tests. However, the current practice of validating data backup restores is only based on requests from clients and there is no defined routine process that would be successful in a restore event.

  DHHS (25%) has not taken sufficient action to implement this recommendation when compared with Treasury and DPAC who have achieved full implementation.

- Implement application-based workstation firewalls, multi-factor authentication for external access and address consultant's concern that the network was poorly segmented (Recommendation 22).

  DHHS had:

  - partially implemented application-based workstation firewalls on its computers and servers that have migrated to Windows 10. Full migration to Windows 10 will take a minimum of two years and the existing Windows 7 computers and servers will not have application firewalls retro-fitted in the interim.
  - implemented multi-factor authentication for external access to a limited extent
  - addressed the IT consultants concerns to some extent due to limited network segmentation.

  DHHS has not taken sufficient action to implement this recommendation.

- Develop a policy to ensure that access to confidential information is valid and that no unused accounts exist that can be wrongfully used, audit access privileges to bring accounts up to date and implement regular testing and monitoring of user access (Recommendation 23).

  DHHS advised that:

  - it has policies for specific systems regarding access to confidential information
  - user accounts are disabled automatically by human resources when staff leave the organisation
  - auditing of access privileges occurs on a system by system basis
  - testing and monitoring of user access is undertaken on a system by system basis.

  DHHS has made limited progress in implementing this recommendation.

- Implement an ICT security plan and associated risk management plan (Recommendation 24).

  DHHS is currently updating its risk management plan in preparation for the development of appropriate ICT security plans.

  DHHS (5%) has made limited progress in implementing this recommendation compared with Treasury and DPFEM who have achieved full implementation and DPAC (75%) who has substantially implemented the recommendation. DPIPWE has not yet commenced implementation.

- Greater use of inbuilt IT controls such as enforcing password standards and controls over the use of unauthorised media (Recommendation 25).

  DHHS advised that:

  - the main source of user authentication is through active directory with enforced password settings by the the Default Domain Controllers Policy
  - password standards are enforced via the ICT Security Policy and handbook where it applies to systems using active directory

- only limited ambulance workstations have group policy blocking on removable media
- build guides for physical Windows servers including domain controllers and remote site servers include settings for disabling user accessible USB ports.

DHHS's (10%) progress in implementing this recommendation is behind that of Treasury (75%).

- Rationalise its incident management system and develop a means of specifically recording and analysing ICT security incidents and near misses (Recommendation 26).

  DHHS (5%) has made limited progress in implementing this recommendation whereas DPIPWE and DPFEM have achieved full implementation.

- While implementing its dual data centre approach, produce business continuity and disaster recovery plans and test them regularly (Recommendation 27).

  DHHS advised that:

  - there are no current disaster recovery plans and a very limited number of business continuity plans, neither of which are tested regularly
  - a lack of resourcing has delayed implementation of this recommendation
  - additional staff are now being recruited to assist with developing DHHS's security framework and implemantation plans.

  DHHS has made limited progress in implementing this recommendation.

DHHS had not implemented one recommendation being to set standards for physical security and implement specific protections accordingly (Recommendation 20). DHHS advised that its network is undergoing significant change and it is awaiting the formation of the ICT security group which will be developing a Security Framework and Implementation Plan before the end of 2018.

DHHS's progress in implementing this recommendation is behind that of DPAC (75%) and DPFEM (50%).

1.4.4 Department of Premier and Cabinet

Eleven recommendations related to DPAC.

DPAC fully implemented three recommendations:

- Back-ups are tested and test documentation retained to provide assurance that restores function correctly (Recommendation 30).
- Enforce password parameters in line with departmental policy (Recommendation 32).
- Modify help-desk systems to enable the recording of security near misses (Recommendation 35).

DPAC partially implemented eight recommendations:

- Outline requirements for varying levels of security and develop guidelines to allow departments to self-assess and accredit departments' various security zones (Recommendation 2).

  DPAC is limiting its investment in current mitigation strategies as its data centres are migrating to cloud services. eGovernment has produced a working sheet to allow departments to self-assess and accredit various security zones. The document has been sent out to all departments and is in the process of data collection. Three years should have provided adequate time to fully implement this recommendation.

- Fully implement at least the 'Top 4' mitigation strategies from the ASD publication: *Strategies to Mitigate Targeted Cyber Intrusions* (Recommendation 5).

  Patching applications and operating system patching have been fully implemented while whitelisting application has not been implemented as DPAC, like Treasury, is still rolling out Windows 10, which will enable whitelisting on all its devices. Minimising administrative privileges has not been fully implemented as DPAC is unable to disconnect staff who have

been seconded to different parts of the organisation and who subsequently return to their former positions.

DPAC (50%) is taking action to address this recommendation but its rate of implementation is less than Treasury (75%) and DPFEM (90%), the same as DPIPWE (50%) and greater than DHHS (10%).

- Upgrade coverage of physical security in its ICT security policy and review construction of server rooms, expand use of CCTV and implement greater hazard protection (Recommendation 28).

  Server rooms are now satisfactorily secured, the use of CCTV has been expanded and greater hazard protection has been implemented. DPAC advised that it is in the process of migrating agency-owned data centre to a Cloud service. Evidence of the implementation of physical security controls in partnership with the building security team was provided.

  However, while DPAC (through eGovernment) is developing a Tasmanian Government cybersecurity policy that addresses physical security, it is still in draft.

  Our expectation was that, by now, any policy addressing physical security would be finalised.

- Set standards for physical security and implement specific protections accordingly (Recommendation 29).

  DPAC is in the process of migrating its agency-hosted servers and ICT infrastructure to a third party provider and is now shifting its focus to documenting procedures for accessing the data centre.

  We accept DPAC's change of emphasis providing the migration of the remaining servers to a compliant third-party provider is completed in the short term.

- Disable local administrator accounts (Recommendation 31).

  DPAC manages and controls its administrator accounts but only by disabling passwords. DPAC advised that it is operationally difficult to re-establish employees' accounts if their accounts have been deleted. This recommendation required more than just password control. So DPAC has yet to fully implement this recommendation.

- Develop a specific ICT security plan (Recommendation 33).

  DPAC's draft ICT security plan uses the template provided by eGovernment. Although DPAC has substantially implemented this recommendation, full implementation could have been achieved.

- Make greater use of in-built IT features such as:
  - time-outs on personal computers
  - enforced password standards
  - controls over unauthorised media and software (Recommendation 34).

  DPAC uses inbuilt IT features such as time-outs on personal computers and enforces password standards. However, it has not implemented controls over unauthorised media and software. DPAC advised that controls over unauthorised media and software will be addressed with the rollout of Windows 10. DPAC has taken sufficient action to implement this recommendation.

- Improve disaster recovery plans by:
  - identifying responsible officers
  - linking to risk management documentation
  - covering security breaches and cyber-attacks
  - setting recovery time objectives
  - further documenting tests of its disaster recovery plan (Recommendation 36).

  DPAC advised that it believes that the IT service delivery models where services are divested through many different supply chains has made disaster recovery plans less relevant and more difficult to simulate. DPAC now utilises many ICT services including cloud, third-party hosting, web proxy, networking, telephony and corporate system support through a variety

of suppliers with their own in-built contingency and disaster recovery plans. DPAC also advised that its remaining ICT infrastructure will be migrated in the coming months.

In so doing, DPAC confirms that its business owners must continue to recognise and understand their business risks, that the IT managers must be involved in the evaluation or services and that vendors must provide detail to satisfy their approach to security, availability (including disaster recovery) and integrity regarding the information and applications.

DPAC maintains that a more contemporary approach to evaluating disaster recovery is needed given these changing factors in the ICT Industry.

DPAC has taken sufficient action to implement this recommendation. However, we saw no evidence that any testing had occurred to ensure continuity of service in the event of an incident.

1.4.5 Department of Police, Fire and Emergency Management

Nine recommendations related to DPFEM.

DPFEM fully implemented four recommendations:

- Document backup and restore procedures and use back up procedures (Recommendation 38).
- Fully document access procedures and implement a regular program of access testing (Recommendation 40).
- Specify in its ICT security plan that risk reviews should take place regularly (Recommendation 41).
- Implement an ICT security incident recording and management and recording system (Recommendation 43).

DPFEM partially implemented five recommendations:

- Fully implement at least the 'Top 4' mitigation strategies from the ASD publication: *Strategies to Mitigate Targeted Cyber Intrusions* (Recommendation 5).

  Whitelisting and operating system patching controls have been fully implemented. However, application patching is not fully automated and administrative privileges have not been fully implemented due to operational requirements.

  DPFEM has substantially implemented this recommendation and has made more progress than the other entities.

- Set standards for physical security and implement specific protections accordingly (Recommendation 37).

  DPFEM was unable to gauge how well its network cabling, routers and switches in remote areas are protected but intends to address this over the next three years through working to meet the requirements of the Australian Government Information Security Manual and Protective Security Policy Framework.

  Due to the number of police stations situated around the State, DPFEM is taking sufficient action to implement this recommendaiton but expects the process to take some time.

- Disable local administrator accounts and implement application-based firewalls (Recommendation 39).

  Firewalls are being used and local administrator accounts are being managed and controlled. However, passwords for accounts are only disabled when a staff member is on transfer and has not left the department.

  DPFEM is working to meet the requirements of the Australian Government Information Security Manual for the management of administration accounts, specifically 'local account controls'. It has a program in place for the lifecycle management of administrator accounts and is working towards assessing options to maintain the current level of functionality to daily policing operations while improving its security.

  DPFEM is taking sufficient action to implement this recommendation.

- Make greater use of inbuilt IT controls such as controls over unauthorised software, media and internet access (Recommendation 42).

  Inbuilt ICT system controls to guard against unauthorised media, software and internet are effective but we were advised that the use of unauthorised media occurs because police require access to specific software to assist in the detection and charging of offenders. Monitoring of the internet, while good at the larger police stations, is more limited in remote areas.

  DPFEM is working to meet the requirements of the Australian Government Information Security Manual. However, we expected DPFEM to have been more proactive in the area of internet monitoring.

- Formalise, implement and test business continuity and disaster recovery plans (Recommendation 44).

  DPFEM has developed a business continuity and disaster recovery plan. While there has been regular testing of individual systems there has been no single over-arching test for the whole system.

  DPFEM is taking sufficient action to implement this recommendation.

1.5 Conclusions

ICT security is a critical risk, the impacts of which have been played out regularly in the media. We expect State entities to place a high priority on addressing this risk and leading the way in the implementation of risk mitigation strategies.

ICT security measures should ensure that all systems are secure and provide a safe environment for government:

- staff to carry out the entity's business
- customers to interact with the entity.

Treasury and DPAC substantially implemented our recommendations and DPFEM is progressing well. DPIPWE and DHHS have yet to fully address ICT security risk.

Recommendations

All entities continually assess the adequacy of their ICT security and ensure resources are allocated to address high risk areas.

1.6 Submissions and comments received

The Premier of Tasmania

The Government is placing greater emphasis on co-ordinating cybersecurity across government and its suppliers with consistent approaches to assessing risk and securing the Government's information and communication technologies.

In recognition of the need to continually improve cybersecurity, the Government allocated ongoing funding in the 2017-18 budget for the Tasmanian Government Cybersecurity Program. Furthermore, the Tasmanian Government Chief Information Officer, appointed in September 2017, is providing strategic leadership of the Government's digital services and cybersecurity.

Will Hodgman MP

Premier

Treasury and Finance

I acknowledge the report and support your conclusion that the Department of Treasury and Finance has substantially implemented the security audit's recommendations.

The report identified that of the eight recommendations, five have been fully implemented and two will be addressed at the conclusion of work already scheduled for completion in mid-2018. In relationto the remaining action (review monitoring of system access by business units across Treasury - recommendation 6), Treasury's ICT security policy assigns responsibility for this function to the relevant business system owners. The Treasury Information Technology Branch confirms this function with the relevant business system owner on a bi-annual basis.

I have noted the recommendation for continual assessment of our ICT Security practices and ensuring resources are allocated to address any high risk areas. Treasury will continue to focus on delivering contemporary ICT services with security measures implemented proportional to any identified risks.

Tony Ferrall

Secretary

Primary Industries, Parks, Water and Environment

DPIPWE has always been committed to hardening its ICT environment and welcomes any information that can help improve ICT security.

The Department has a strong operational security record and is continuing with the program of works that are already underway to deliver the remaining items identified by TAO. The Department's program of ICT security-related activities is not limited to addressing the recommendations of the Audit, but includes working closely with the Office of eGovernment (Department of Premier and Cabinet) to align with Whole of Government security directions. As part of this, DPIPWE is working to be compliant with International standards 27001 and 31000.

With respect to the 10 specific recommendations relevant to DPIPWE, the following management responses are provided:

Recommendation 5: Fully implement at least the 'Top 4' mitigation strategies from the ASD publication: Strategies to Mitigate Targeted Cyber Intrusions.

Response: The response below separately addresses the recommendations for each of the ASD top four:

ASD Recommendation 1 (application whitelisting)
DPIPWE has progressed the implementation of application whitelisting through setting up a trial involving three branches of the Department. After assessing and mitigating any issues identified in the trial, DPIPWE will continue rolling out the full implementation, which is scheduled to be completed in 2018.

ASD Recommendation 2 (patching applications)
DPIPWE currently patches mainline and high risk applications such as Microsoft, Adobe software, ArcGIS, Google Earth etc. The Department will continue to perform such patching in a timely manner with DPIPWE's System Centre Configuration Manager (SCCM).

ASD Recommendation 3 (patching operating system)
Operating system patching has been implemented.

ASD Recommendation 4 (Minimising users with administrative privileges)
Minimising administrative privileges has been implemented.

Recommendation 10: Update the ICT security policy and upgrades access controls, alarms and hazard protection at specific server rooms.

Response: The ICT equipment in the identified server room will be moved to a secure third party data centre in 2018/2019.

Recommendation 11: Provide protective covering for exposed building cabling and provide basic security of switches and routers.

Response: The identified fibre optic cabling is located in a secure area but it will also be securely covered by the end of June 2018.

Recommendation 12: Provide off-site storage for all backup tapes. Backup procedures should be recorded and testing logs maintained.

Response: DPIPWE recognises that improvement can be made in backup storage and is working to move the backup tapes from separate buildings to fully offsite by August 2018.

Recommendation 13: Install firewalls to all workstations and disable local administrative accounts

Response: No local administrator accounts are granted by default in DPIPWE. Full disabling of local administration accounts would have a high impact on IT support operations, however DPIPWE will review the current group policies (which control administrative rights) and alter current group policies based on risk analysis to the Agency.

Recommendation 14: Develop a policy to ensure access to confidential information is valid and ensure no unused accounts exist. Implement regular testing and monitoring of user access.

Response: DPIPWE has made considerable progress with this recommendation and will continue to implement the policy. Documentation of staff termination procedures is well advanced and will be completed by July 2018.

Recommendation 15: Implement an ICT security plan and associated risk management plan

Response: DPIPWE has worked closely with the Office of eGovernment contributing to a range of security policies and from this base will now develop security policies applicable to DPIPWE, adopting the international standards for information security: ISO/IEC 27001, and for risk management: ISO 31000.

Recommendation 16: Implement inbuilt controls over the use of unauthorised media

Response: DPIPWE uses in-built IT features such as time-outs on personal computers and enforces password standards. The Department has already started a trial to test the impacts of the introduction of controls over the use of unauthorised media. DPIPWE will consider the introduction of appropriate controls over unauthorised media and software with the future rollout of Windows 10.

Recommendation 17: Implement an ICT security incident recording and management system

Response: DPIPWE has fully implemented this recommendation

Recommendation 18: Develop business continuity plans and ICT security disaster recovery plans and test plans regularly

Response: DPIPWE has a resilient architecture designed to cater for disasters but does acknowledge the need for a disaster recovery plan to formalise the processes. DPIPWE has prioritised the development of the disaster recovery plan by July 2018.

Development of a Business Continuity Plan is a large undertaking and DPIPWE has already taken the first steps by capturing the recovery priorities of applications used by business units. Further, agency wide work will continue to finalise a Business Continuity Plan in 2018.

John Whittington

Secretary

Health and Human Services

The Department of Health and Human Services' response to recommendations 5, 19-27 are detailed below.

Recommendation 5: We recommend the DHHS fully implement at least the ASD 'Top 4' mitigation strategies from Strategies to Mitigate Targeted Cyber Intrusion

Upon review suggest modification to reflect recent activity as the Department is more advanced than indicated, i.e. this work is approximately 37% completed.

Recommendation 19: We recommend the DHHS upgrades access controls, alarms and hazard protection at specific server rooms where necessary

Agree in principle however request that the method of calculation be reviewed as the current method does not take into consideration risk to the majority of the computer and storage infrastructure which has been mitigated by using the whole-of-Government Datacentre-as-a-service (DCaaS) contracts. 82% of the virtual machine fleet (1121 total as at May 2018) and 55% of the physical server fleet which host the department core and critical applications, systems and network are hosted in the WoTG DCaaS datacentres in contrast to the 33% rating that was given in the report.

Recommendation 20: Sets standards for physical security and implements specific protections accordingly

Upon review suggest modification to reflect recent activity as the Department is more advanced than indicated, i.e. this work has commenced and is approximately 5% completed.

Recommendation 21: We recommend the DHHS tests backups at a frequency commensurate with risk

Agree in principle with the report's review on progress performance.

Recommendation 22: We recommend the DHHS:

- **Implement application-based workstation firewalls**
- **Implement multi-factor authentication for external access**
- **Address its consultant's concern that the network was poorly segmented**

Agree in principle with the report's review on progress performance.

Recommendation 23: We recommend the DHHS:

- **Develop a policy to ensure that access to confidential information is valid and that no unused accounts exist that can be wrongfully used**
- **Audit access privileges to bring accounts up to date**
- **Implements regular testing and monitoring of user access**

Upon review suggest modification to reflect recent activity as the Department is more advanced than indicated, i.e. this work has commenced and is approximately 30% completed.

Recommendation 24: We recommend the DHHS implements an ICT security plan and associated risk management plan

Agree in principle with the report's review on progress performance.

Recommendation 25: Makes greater use of inbuilt IT controls such as enforcing password standards and controls over use of unauthorised media

Upon review suggest modification to reflect recent activity as the Department is more advanced than indicated, i.e. this work has commenced and is approximately 25% completed.

Recommendation 26: Rationalises its incident management system and develops a means of specifically recording and analysing ICT security incidents and near misses

Agree with the report's review on progress performance.

Recommendation 27: While DHHS implements its dual data centre approach, the Department should produce business continuity and disaster recovery plans and test them regularly

Agree in principle with the report's review on progress performance.

Michael Pervan

Secretary

Premier and Cabinet

I acknowledge the report and support your conclusion that the Department of Premier and Cabinet (DPAC) has substantially implemented the security audit's recommendations.

I have noted the recommendations for continual assessment of the ICT Security practices and ensuring resources are allocated to address high risk areas. The report's recognition of recent developments, particularly in relation to adopting a risk-based approach, is welcomed. DPAC will continue in its aim to deliver ICT services that are secure, but also practical, achievable and proportional to the risks presented in DPAC.

The report identified that many control measures for ICT Security at DPAC are progressing well. The need to accelerate the collation of these actions into the ICT Security Plan is noted and being actively progressed.

You will have also noted the increase in collaboration and sharing of resources in the Tasmanian Government being driven by DPAC's Office of eGovernment under the leadership of the Tasmanian Government Chief Information Officer. This community of practice is leading to greater outcomes and improved efficiency regarding our approach to ICT Security which DPAC staff fully participate in.

DPAC's Information and Technology Services branch will continue to work with DPAC's Office of eGovernment to align these policies, practices and plans to ensure DPAC's approach to information and cyber security is consistent with the whole-of-government approach.

Jenny Gale

Secretary

Police, Fire and Emergency Management

The Department does not feel it necessary to add further comment in relation to the report.

Donna Adams

Acting Secretary

2. TASMANIAN MUSEUM AND ART GALLERY: COMPLIANCE WITH THE *NATIONAL STANDARDS FOR AUSTRALIAN MUSEUMS AND GALLERIES*

2.1 Background

TMAG is the second oldest museum in Australia and collects, preserves, researches, displays, interprets and safeguards physical evidence of Tasmania's natural and cultural heritage, together with relevant material from interstate and overseas. It does this at multiple sites around Hobart, including the city waterfront site, the herbarium at the University of Tasmania, a restoration and storage site at Moonah and a research and storage facility at Rosny.

TMAG's waterfront site had undergone a partial (Stage 1) redevelopment shortly before the 2015 audit. Stage 1 opened in March 2013 and includes new public and exhibition spaces, a centralised visitor services hub and a new café. Visitors can now experience more of the waterfront site, including a range of nationally significant archaeological material[4]. However, much of TMAG's collection is still in storage.

At the time of the 2015 audit, TMAG resided within State Growth and had a Board of Trustees (Board) that held the museum's collections in trust for the people of Tasmania. TMAG was answerable to the Governor through the Minister for the Arts.

In 2013–14, there were 487 000 visitors over the 12-month period (the year Stage 1 of the redevelopment opened). This was significantly higher than the typical 300 000 visitors prior to the redevelopment[5]. In 2016–17, the total number of visitors to TMAG was just over 415 000[6].

In 2013, a national taskforce comprising representatives from each jurisdiction, plus the Collections Council of Australia, published Version 1.3 of the National Standards for Australian Museums and Galleries (National Standards). These standards 'focused on key areas of activity common to organisations that care for collections and provide collection-based services to the community'.

The objective of the 2015 audit was to express an opinion on TMAG's compliance with the National Standards.

The scope of the audit was confined to TMAG and did not include the Queen Victoria Museum and Art Gallery in Launceston or other smaller museums and galleries across the State.

2.2 Conclusions from the 2015 audit

The main findings of the 2015 audit were that TMAG:

- had an unclear legal and management framework. Roles and responsibilities between TMAG and State Growth needed to be reviewed and clarified
- had a number of key documents required under the National Standard but lacked a forward (strategic) plan. Consequently, we did not believe TMAG was effectively managed regarding key policies and plans. With regard to information and risk management, TMAG generally performed well
- had undertaken a visitor survey in recent years but we were not persuaded that information about visitors was being evaluated to assist with future planning as required by the National Standards. TMAG also did not have a forward plan, which was needed to outline strategic objectives and to identify strategies for attracting new and existing audiences. We concluded that TMAG could further increase its customer focus
- did not have an appropriate rationale for presenting its collection, which we expected would reside in the interpretation strategy and be guided by higher-level documents such as the statement of purpose and the forward plan. There was also inadequate significance

4. Discover Tasmania, Discover Tasmania: Attraction, http://www.discovertasmania.com.au/attraction/tasmanianmuseumandartgallery, Accessed 18 July 2014.
5. Tasmanian Museum and Art Gallery, Annual Report 2010-2011, State of Tasmania, 2011, p.8.
6. Tasmanian Museum and Art Gallery, Annual Report 2016-2017, State of Tasmania, 2017, p.4.

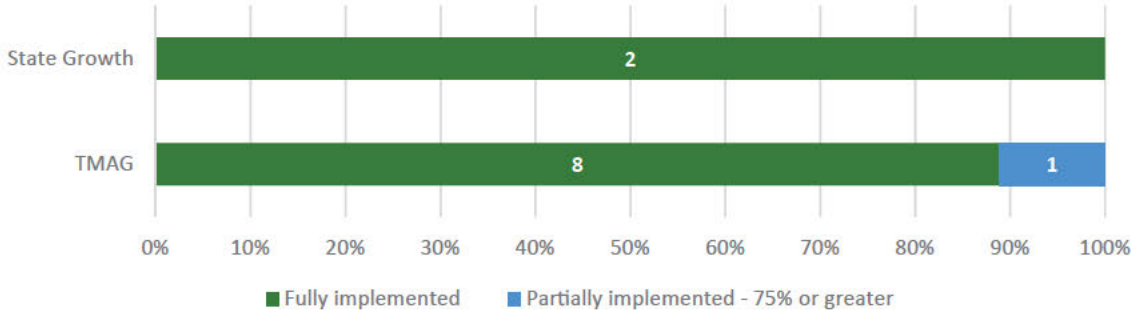
documentation of TMAG's collection. However, some exhibits were changed on a regular basis, although a benchmark would help to determine rotation frequency

- preserved and stored the vast majority of its significant collections soundly, with training undertaken to ensure collections were properly handled. However, exceptions to this were:
    - the Moonah facility, where environmental conditions, cleaning and pest management were poor (largely mitigated by storage of more robust items)
    - lack of policies and procedures for security measures applied to different exhibits and there were inconsistencies in the security measures applied.

2.3 Status of recommendations

The 2015 audit resulted in 11 recommendations. Figure 2 shows our assessment of the extent to which the recommendations have been implemented.

Figure 2: Extent of recommendation implementation



The implementation status of the recommendations is summarised in Table 2 below.

Table 2: State Growth and TMAG — status of implementation of recommendations

No.	Recommendations (abbreviated)	State Growth	TMAG
1	Review the *Tasmanian Museum Act 1950* and examine alternative governance models	✓	
2	The *Tasmanian Museum Act 1950* review clarifies the roles and responsibilities of the Minister, the trustees and State Growth	✓	
3	Create a forward plan to ensure strategic aims and objectives are clearly articulated		✓
4	Ensure the risk register addresses risks associated with long-term funding requirements for Redevelopment Stage 2		✓
5	Undertake annual surveys to determine visitor satisfaction and visitor preferences and use this information to inform the creation of exhibitions		✓
6	Develop a forward plan, which includes strategic objectives, long and short-term goals and an action plan that identifies clear strategies to retain existing and attract new audiences		✓
7	Develop a forward plan and interpretation strategy to ensure an appropriate rationale for presenting the collection		✓

No.	Recommendations (abbreviated)	State Growth	TMAG
8	Undertake a risk assessment of its collection to determine the extent to which significance documentation is required for items acquired before 2010 to ensure the most significant items are displayed and optimal security and preservation of the collection is achieved		**P** (80%)
9	Develop a collection rotation benchmark		✓
10	Create clear guidelines of security measures to assist staff in ensuring the continuing safety of its displayed exhibits		✓
11	Develop a formal process to identify training needs in relation to moving and handling of the collection		✓
	No. of recommendations	**2**	**9**

✓ Fully implemented, × Not implemented, **P** Partially implemented (%), Blue shading - not applicable.

Our findings in relation to each entity are detailed below.

2.3.1 Department of State Growth

State Growth was responsible for implementing two recommendations and both had been fully implemented:

- Review the *Tasmanian Museum Act 1950* and examine alternate governance models (Recommendation 1).

  A review of the legislation was undertaken resulting in it being repealed and replaced by the *Tasmanian Museum and Art Gallery Act 2017* (TMAG Act) in October 2017.

- Clarify the roles and responsibilities of the Minister, the trustees and State Growth (Recommendation 2).

  The new Act not only established a new governance model but also clarified the roles and responsibilities of the Minister, the Trustees and State Growth.

  The following changes to the governance and operational structure were noted:

  - the Minister now has the power to appoint the Trustees. The Minister can also deliver a statement to the Board outlining the Minister's expectations of TMAG and the Board. The Minister may also deliver Ministerial Directions to the Board that must be complied with.
  - the Board is now appointed by the Minister rather than the Governor. In making Board appointments, the Minister consults and seeks nominations from the Royal Society of Tasmania and from the broader Tasmanian community.
  - the functions of the Board have now been clearly defined in the TMAG Act as:
    - having strategic oversight of TMAG
    - oversight of control and management of TMAG
    - stewardship of TMAG's collections.
  - the role of Director has now been defined as being responsible to the Board for the general administration and management of TMAG.
  - staff employed by TMAG are appointed under the *State Service Act 2000*.

2.3.2 Tasmanian Museum and Art Gallery

TMAG was responsible for implementing nine recommendations.

TMAG fully implemented eight recommendations:

- Implement a strategic plan covering the period 2016–21 (Recommendation 3).

  The plan articulates its aims and objectives by stating that its outcomes for the period are covered by the following four strategic outcomes:

  - a welcoming physical and virtual destination
  - strong collections that tell Tasmania's story
  - an involved community
  - transformational use of resources.

- Note long-term funding issues in the risk register (land, buildings and infrastructure) (Recommendation 4).

  Mention has also been made in TMAG's 2016 strategic asset management plan of its intention to eventually fulfil Stage 2 of the 2008 Master Plan Development, although how Stage 2 will be funded is not included.

- Undertake visitor surveys (Recommendation 5).

  A consultant is now engaged to undertake the surveys and this has allowed TMAG to identify its audience profile and understand its audiences' key motivators. For instance, for 2015–16, the consultant's report noted that:

  - interstate visits are now in the majority
  - TMAG has successfully focussed on families as a priority audience
  - younger audiences have increased
  - exhibitions are attracting more visits[7].

  The survey is undertaken annually although the 2017 survey or outcomes was not available at the time of our audit.

- Develop a forward plan, which includes strategic objectives, long and short-term goals and an action plan that identifies clear strategies to retain existing audiences and attract new visitors (Recommendation 6).

  TMAG also finalised its 2018-21 Engagement Strategy in 2018, which uses the results of audience surveys to frame its forward engagement strategies, for example, using large-scale programs such as festivals to increase family audiences.

- Develop a forward plan and interpretation strategy to ensure an appropriate rationale for presenting the collection (Recommendation 7).

  A draft Interpretation Strategy was developed in 2009, which we concluded in 2015 was not an appropriate rationale for presenting the collection given that, at that time, it was still in draft form. Since then, the draft strategy has been finalised and was reviewed in December 2017. Further detail on the Interpretation Strategy is contained below.

- Develop a collection rotation benchmark (Recommendation 9).

  Our 2015 audit identified that TMAG regularly rotated its collection, however, there was no benchmark as to the appropriate level of exhibition rotation to attract new visitors. In assessing TMAG's implementation of this recommendation, we now acknowledge that a numerical rotation benchmark is not useful in determining what a museum should exhibit.

  Most museums establish policies or guidelines that encompass various aspects of collection management, such as how the collection is cared for and how it is made available to the public. Exhibition or interpretation policies reflect the type of collection a museum holds and complement the goals articulated in museum strategic plans. Such policies usually address:

7. Morris Hargreaves McIntyre, Moving forward, *Tasmanian Museum and Art Gallery Visitor 360° annual report August 2016*.

- the process undertaken when an object is chosen to be in an exhibition
- the nature of the material, its condition and the types of deterioration to which the object is susceptible
- exhibition of in-house items or loan items
- safety and security of the exhibition
- remedial preparation
- facilities or environment for the exhibition
- communication with cultural representatives
- engaging visitors and users
- funding
- period of display
- schedule for the refreshment and renewal of the exhibitions.

TMAG prepared an Interpretation Strategy (updated December 2017) which is intended to guide program development and inspire interpretive outcomes. It covers a variety of areas from the larger whole-of-site exhibition plan to approaches to object interpretation. TMAG uses this strategy to inform new museum programs and exhibitions and support future program development.

TMAG decided against a chronological and identity gallery-led exhibition approach and elected to deliver theme and story-led interpretation that is object rich with multiple layers of engagement. As resources do not allow TMAG to change major galleries regularly, it aims to refresh spaces by changing objects or stories. Programs are developed to be updateable with a process for object and story rotation in place. This approach also takes into account collection care, changes to information and stories, the representation of all of Tasmania and changing individual points of entry to include stories and objects from many regions and communities without disrupting the larger story or theme. TMAG also strives to maintain contemporary methods and styles of communication.

We are satisfied that the Interpretation Strategy, together with the TMAG strategic plan 2016-21, satisfies the intent behind our original recommendation.

- Create clear guidelines of security measures to assist staff in ensuring the continuing safety of its displayed exhibits (Recommendation 10).

  TMAG has established clear guidelines of security measures to ensure continuing safety of its displayed exhibits. TMAG undertakes a preservation needs assessment and has set out a five year plan for conservation on a collection and display priority basis to comply with legislation, industry best practice and the National Standards.

- Develop a formal process to identify training needs in relation to movement and handling of the collection (Recommendation 11).

  Training is held annually and picks up staff requiring refresher courses as well as new staff. A spreadsheet tracks new and existing staff to ensure collection handling training is kept up-to-date.

TMAG partially implemented one recommendation being to undertake a risk assessment of its collection to determine the extent to which significance documentation[8] was required (Recommendation 8).

'Significance' refers to the values and meanings that items and collections have for people and communities. Significance may also be defined as the historic, artistic, scientific and social or spiritual values that items and collections have for past, present and future generations. These are the criteria or key values that help to express how and why an item or collection is significant.

8. The National Standards require the significance of collection items should be investigated and documented.

Significance assessment is the process of researching and understanding the meanings and values of items and collections. The assessment process explores all the elements that contribute to meaning, including history, context, provenance, related places, memories and comparative knowledge of similar items. It goes beyond a conventional catalogue description to explain why and how the item is important and what it means. The results of the analysis are synthesised in a statement of significance which is a reasoned, readable summary of the values, meaning and importance of an item or collection. It is a means of sharing knowledge about why an item is important and why it has a place in a public collection.

TMAG has been undertaking significance assessments on a thematic and research basis so the notion of risk is not an overarching consideration in this process. A thematic or research assessment basis recognises that an individual item may have characteristics which make it important to many groups or collections, meaning it would have multiple significance assessments undertaken. Conversely, groups of items may be covered by a single significance assessment, which means there are multiple ways of expressing and documenting the significance aspects.

Undertaking and documenting significance assessments is not a quick process. TMAG has estimated it has 250 000 significance assessments to make, which may take many years to complete.

We are satisfied TMAG is taking significant action to implement this recommendation.

2.4 Conclusion

We are pleased to confirm that:

- State Growth has fully implemented the recommendations
- TMAG has fully implemented eight recommendations and has made significant progress on implementing the remaining recommendation.

2.5 Submissions and comments received

State Growth

I can advise that there are no management comments that we wish to make regarding the Tasmanian Museum and Art Gallery (TMAG) audit report. Following the report we have fully implemented the recommendations, TMAG has fully implemented eight recommendations and significant progress has been made on the remaining recommendation.

There are no further matters that we wish to raise about findings and recommendations of the report.

Kim Evans

Secretary

Tasmanian Museum and Art Gallery

The Director, Ms Janet Carding, while not offering any overal comment on the report, requested a minor amendment, which we agreed to.

3. NUMBER OF PUBLIC PRIMARY SCHOOLS

3.1 Background

With declining rural populations, the decision on whether to close schools has been an issue across Australia and Tasmania is no exception, with the number of publicly funded schools with low enrolments of concern to government.

From 1996 to 2010, there was a 7% reduction in the number of full-time students enrolled at Tasmanian primary schools and an 11.7% reduction at public primary schools[9]. In 2011, the Treasurer stated in the budget speech[10] that many [schools] also have under-utilised classrooms due to falling school populations and that if we do not act now, Tasmanian schools will be filled to less than 60% of their capacity by 2013.

Subsequently, the government identified 20 schools for closure as part of its budget savings measures for the 2011 state budget. However, following community backlash to that process, the decision was made not to close any of the schools. Instead, the Minister for Education and Skills established the School Viability Reference Group in August 2011 to consult widely with the community and to provide recommendations on the provision of a viable public school system in Tasmania. The resulting Ministerial Report — *School Viability Reference Group Report* (School Viability Report) was provided to the Minister in January 2012 and was a significant input into our 2015 audit.

The objective of the audit was to form an opinion on the efficiency and effectiveness of the number and location of public primary schools in Tasmania.

The scope of the original audit was limited to primary schools (and the primary component of district schools) as at January 2014, on the basis that there were considerably fewer secondary schools (28) than primary or combined schools (151), which we saw as a potential indicator of an oversupply.

3.2 Conclusions from the 2015 audit

The main findings of the 2015 audit were that:

- There were some counter-intuitive results that suggested that Tasmania's average enrolments per school and proportion of small schools was not unreasonable when the State's low urbanisation was considered. There was also no evidence that small schools were disadvantaged in terms of educational performance.
- On the other hand, Tasmania had:
    - a high cost per student compared to the Australian average. The difference was due to higher staff to student ratios, particularly in smaller schools
    - high levels of unused capacity
    - only a small proportion of schools with enrolments in the 300 to 500 range favoured by experts.

  With each closed school potentially saving the government $433 000 per annum, we concluded that DoE had too many primary schools, particularly in rural areas.

  We identified six schools for which a strong case existed for closure:
    - Edith Creek Primary School
    - Geeveston Primary School
    - Clarendon Vale Primary School
    - Avoca Primary School
    - Risdon Vale Primary School
    - Sprent Primary School.

9. Australian Bureau of Statistics, *Regional Population Growth, Australia, Schools, Series 4221.0*, ABS, Canberra, 2010.
10. L Giddings, *2011-12 Budget Speech, 'Strong decisions Better future'*, delivered in the House of Assembly on 16 June 2011 on the Second Reading of the Consolidated Fund Appropriation Bill (No 1) 2011.

We also identified another 11 schools with a moderate case for closure:

- Redpa Primary School
- Warrane Primary School
- Collinsvale Primary School
- Natone Primary School
- Zeehan Primary School
- Riana Primary School
- Hillcrest Primary School
- Kempton Primary School
- Sandy Bay Infant School
- Sassafras Primary School
- Springfield Gardens Primary School.

- Despite the lack of a systematic review process, there had been a satisfactory level of review over the past five years. In addition, the recommendations of the School Viability Report had received a reasonable level of attention.

3.3 Status of recommendations

The 2015 audit report contained seven recommendations, all of which were originally directed at DoE. However, Recommendation 4 also suggested that individual schools perform an annual assessment of the adequacy of the range of educational experiences offered at each school.

The implementation status of the recommendations is summarised in Table 3 below.

Table 3: Number of public primary schools — status of implementation of recommendations

No.	Recommendations (abbreviated)	DoE
1	Review whether more staff per student than other Australian jurisdictions is needed	✗[a]
2	Continue to encourage mergers and closures of schools where students would not be disadvantaged by long travel times	✗[a]
3	Regularly review the need for additional capacity where occupancy exceeds 90%	✓
4	Perform annual assessments of the adequacy of the range of educational experiences offered at each school	✗[a]
5	Further analyse and consult on the viability of listed schools and, where appropriate, actively encourage closures or mergers	✗[a]
6	Introduce an annual review of the viability of all DoE schools	✗[a]
7	Actively target and encourage school communities to consider mergers and closures based on an annual review of school viability	✗[a]
	Number of recommendations	**7**

✓ Fully implemented, ✗ Not implemented.
(a) Not proceded with due to Government policy of no forced school closures.

In responding to our original audit, the Secretary stated:

> *The recommendations contained within the report are noted and the Department will take these into consideration for future planning, where it assists in the delivery of government policy.*

In responding to the self-assessment questionnaire on 28 September 2017, as part of our current audit, the then Secretary advised:

> *The Government has a policy of 'no forced school closures' which affects the extent to which the Department undertakes the systematic reviews recommended in the Report. The Government-supported model for maintaining viable, high performing schools continues to be the School Transition Fund (STF) which assists schools to voluntarily review education delivery in their region.*

In relation to Recommendation 3 – regularly review the need for additional capacity where occupancy exceeds 90% – we were advised that DoE closely monitors capacity at all government schools through its Asset Strategy Steering Committee (ASSC). All schools at, or above, 85% were recently referred to the ASSC. Identification of a school as having capacity issues initiates a site visit and investigation. DoE explained that it is currently developing an education infrastructure planning framework to aid its strategic understanding of current and projected capacity issues and is also proposing to implement an asset management system to manage and monitor information including capacity.

The Secretary also provided comments on how DoE had addressed, in a manner consistent with government policy, the recommendations from the 2015 report. These comments are summarised in the Submissions and Comments Received section below:

3.4 Conclusion

In recognition of the current government policy of no forced school closures, we accept the position taken by DoE to not implement most of the recommendations in our 2015 report.

3.5 Submissions and comments received

Department of Education

Review whether more staff per student than other Australian jurisdictions is needed (Recommendation 1).

- DoE does not actively review whether it needs to have more staff per student than other Australian jurisdictions. However, data from the Australian Bureau of Statistics[11] shows that in the Tasmanian Government School sector, there has been a slight decrease in the student to teaching staff ratio from 2015 to 2016 at the primary school level, as well as across all levels generally.
- Tasmania's above-average staff to student ratios largely reflect above-average spending on non-teaching staff and on other operating costs.
- The relatively high level of non-teaching staff per child reflects DoE's decision to allocate staff for specialised services (such as disability, psychology and social services) to deliver in-school services due to the high level of need in many Tasmanian schools.

11. Catalogue number 4221.0 – Schools, Australia, 2016: Table 53a student (Full Time Equivalent) to teaching staff (Full Time Equivalent) ratios, 2001-2016.

Continue to encourage mergers and closures of schools, where students would not be disadvantaged by long travel times (Recommendation 2).

- The government-supported model for maintaining viable, high performing schools is the School Transition Fund (STF). The STF was created in 2013 to support school communities in moving towards streamlining educational provision and strengthening the education system in a cost effective way.
- The STF provides opportunities for school communities to voluntarily look at potential changes in education delivery in their region. Schools are supported by DoE when they enter into these conversations with their communities. Final agreements on any changes in education delivery are transparent and made jointly with the individual school community.
- Since the start of the STF in 2013 until the end of 2016, the accumulative saving achieved through amalgamations is approximately $7.9 million. Of this, approximately $4.6 million has been saved through staffing budget allocation as a result of school closures, mergers and amalgamations. In addition, approximately $804 000 has been saved through the School Resource Packages (SRP) budget as a result of school closures, mergers and amalgamations.

Perform annual assessments of the adequacy of the range of educational experiences offered at each school (Recommendation 4).

- Schools report on their education provision and their success through their annual reporting. All schools are committed to a process of continuous improvement and make local decisions about the range of educational experiences offered.
- School principals are supported in planning and implementing improvement processes by Principal Network Leaders.
- DoE's Performance and Development Framework, applicable to all permanent employees, is closely aligned with school improvement planning and processes.
- DoE is confident all government schools are in a position to provide at least an adequate range of educational experiences.

Further analyse and consult on the viability of listed schools and where appropriate actively encourage closures or mergers (Recommendation 5).

- The government-supported, voluntary approach to school mergers and closures is discussed under Recommendation 2 above.
- The Department recognises that the viability of schools is a highly emotive issue, especially for school communities that have been named as potentially unviable more than once.
- It should be noted that one of the six schools identified in the Report as having a 'strong case for closure' – Edith Creek Primary School in the state's North-West – has in fact achieved a significant growth in student numbers, from 39 students full-time equivalent (FTE) in 2014 to 56 (FTE) in 2017, an increase of approximately 38%.

Introduce an annual review of the viability of all schools (Recommendation 6).

Refer to the responses provided to Recommendations 2 and 5 above.

Actively target and encourage school communities to consider mergers and closures based on an annual review of school viability (Recommendations 7).

Refer to the responses provided to Recommendations 2 and 5 above.

Jenny Gale

Secretary

4. ROAD MANAGEMENT IN LOCAL GOVERNMENT

4.1 Background

At the time of our original audit in 2015, Tasmania had approximately 24 000 km of roads. Local government (councils) controlled 14 300 km of sealed and un-sealed roads representing 69% of total infrastructure held by councils with an estimated value of $3.243bn[12].

Councils can construct their own roads but usually acquire new roads from property developers, for example, on completion of a property sub-division. Across the local government sector generally, contractors construct new roads and councils use their own workforce to maintain the roads. Maintenance, renewals and upgrades are funded from councils' general revenue as well as from grants, predominantly from the Commonwealth Government.

The objective of our 2015 audit was to express an opinion on whether councils were managing the construction and maintenance of council-owned roads efficiently and effectively. We examined the management of sealed and unsealed roads (excluding bridges) by:

- Central Highlands Council (CHC)
- Devonport City Council (DCC)
- Northern Midlands Council (NMC)
- Waratah-Wynyard Council (WWC).

4.2 Conclusions from the 2015 audit

The main findings of the 2015 audit were that:

- CHC, DCC and WWC roads were either in a reasonable or satisfactory condition, while NMC roads were considered to be in a good condition
- CHC, DCC and WWC were either reasonably or relatively efficient compared to other councils and were performing an appropriate level of maintenance. The report noted that NMC may have been less efficient in comparison
- none of the four councils adequately reported on road conditions or the sustainability of their road networks
- DCC and WWC needed to review the level of renewal and upgrade to sustain the quality of their road networks in the future
- CHC did not have effective processes to ensure that complaints were actioned in a timely manner or to ensure the timely renewal and upgrade of ageing assets
- DCC had effective processes to identify and fix maintenance issues and identify and program required renewals and upgrades but there were some indications of a need to review the level of renewal and upgrade to sustain the quality of the road network in the future
- WWC documentation of the complaints, inspection and renewal programs was deficient.

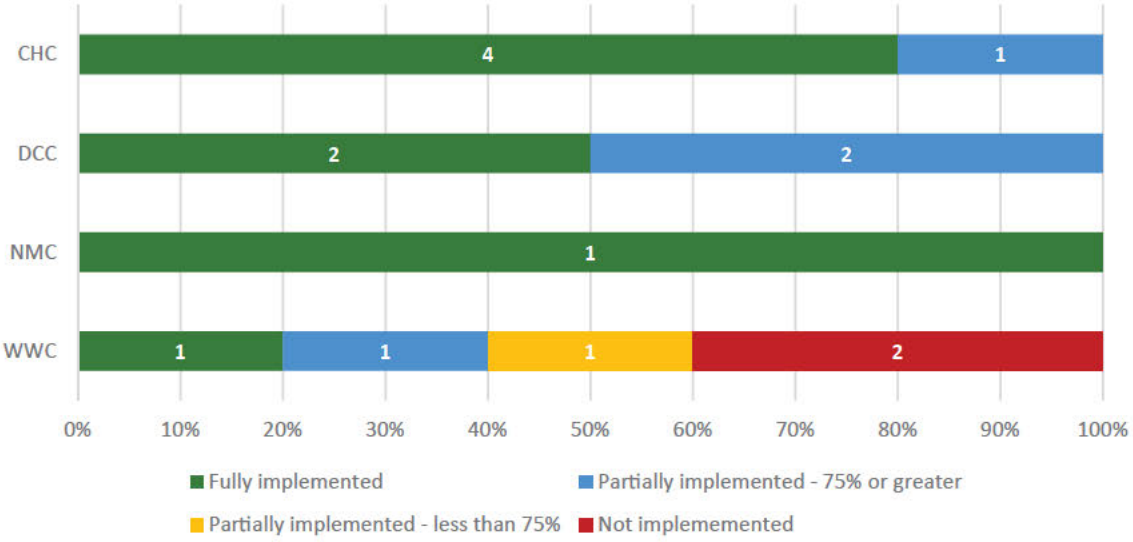
4.3 Status of recommendations

The 2015 audit resulted in 15 recommendations. Figure 3 shows our assessment of the extent to which the recommendations have been implemented.

12 Tasmanian Audit Office, *Report of the Auditor-General No.7 of 2014–15, Auditor-General's Report on the Financial Statements of State entities, Volume 4 Local Government Authorities and Tasmanian Water and Sewerage Corporation Pty Ltd 2013–14, Part I, Key Points, Joint Authorities, TasWater and Other Matters*, TAO, Hobart, 2015, p54.

The degree of implementation of recommendations for this audit is timely as we will shortly commence planning for a similar audit focussing on State-owned roads.

Figure 3: Extent of recommendation implementation



The implementation status of the recommendations is summarised in Table 4 below.

Table 4: Road management in local government — status of implementation of recommendations

No.[a, b]	Recommendations (abbreviated)	CHC	DCC	NMC	WWC
1	Re-establish procedures to ensure the complaints system is an effective component of the maintenance program	✓			
2	Include dates for the end of remaining useful life of each asset in the asset register	✓			
3	Review condition assessments in the asset register to ensure they reflect reality	✓			
4 9 10 15	Provide indicators of road condition and commentary on sustainability ratios in its annual report	**P** 75%	✓	✓	✗
5	Provide regularly-updated information on website about hazards and roads in poor condition	✓			
6 12	Monitor and document progress of road inspection program		✓		✗
7	Update and revise the 2011 asset management plan to improve long-term planning		**P** 80%		
8 14	Review the expenditure level on renewal and upgrade of roads which considers the estimated lives of roads, because of their impact on sustainability ratios		**P** 80%		**P** 90%

No.[a, b]	Recommendations (abbreviated)	CHC	DCC	NMC	WWC
11	Improve the system used to record complaints and action requests and investigate ways to reduce resolution times				✓
13	Document decisions to defer capital works and update subsequent renewal dates in the asset register				**P** 25%
	Number of recommendations	**5**	**4**	**1**	**5**

✓ Fully implemented, × Not implemented, **P** Partially implemented (%), Blue shading - not applicable.

Notes: *(a) Multiple recommendation numbers in each row arise where the same recommendation has been made separately for each entity in the original report*

(b) Recomendation number in original report

4.3.1 Central Highlands Council

Five recommendations related to CCH.

CCH fully implemented four recommendations:

- Re-establish procedures to ensure the complaints system is an effective component of the maintenance program by implementing new complaints procedures, which requires the complaint to be entered electronically (Recommendation 1).
- Include dates for the end of remaining useful life of each asset entered in the asset register (Recommendation 2).
- Review condition assessments in the asset register to ensure they reflect reality have been undertaken with the next condition assessment due in the 2018–19 financial year (Recommendations 3).
- Regularly provide updated information on the CHC website about hazards and roads in poor condition (Recommendation 5).

CHC partially implemented one recommendation:

- Provide indicators of road condition and commentary on sustainability ratios in its annual report (Recommendation 4).

  While CHC was publishing road condition and sustainability ratio information in its annual report, it lacked explanatory commentary. Consequenty, CHC is yet to fully implement this recommendation.

4.3.2 Devonport City Council

Four recommendations related to DCC.

DCC fully implemented two recommendations:

- Monitor and document progress of the road inspection program through the use of a diarised inspection program that is updated when the work has been completed (Recommendation 6).
- Provide indicators of road condition and commentary on sustainability ratios in the annual report and annual plan (Recommendation 9).

DCC partially implemented two recommendations:

- Update and revise the 2011 asset management plan to improve long-term planning (Recommendation 7).

  DCC prepared a 2017 draft transport asset management plan that will feed into its draft road network strategy. However, the plan and strategy are still in draft form.

- Review the expenditure level on renewal and upgrade of roads which considers the estimated lives of roads, because of their impact on sustainability ratios (Recommendation 8).

  DCC has prepared a draft transport asset management plan detailing expenditure on asset maintenance/renewal/new over the 10 years from 2018 to 2027. While we cannot independently assess the level of expenditure on DCC's roads over the period covered by the asset management plan, the plan states DCC's present funding levels on transport infrastructure are sufficient.

  While the information contained in DCC's transport asset management plan satisfies our recommendation, it will be fully implemented when the plan is finalised.

4.3.3 Northern Midlands Council

NMC fully implemented its only recommendation being to provide indicators of road condition and commentary on sustainability ratios in the annual report (Recommendation 10).

NMC's annual plan contains details of the performance measures and its annual report contains details of the sustainability ratios and commentary on the condition of roads.

4.3.4 Waratah Wynyard Council

Five recommendations related to WWC.

WWC fully implemented one recommendation being to improve the system used to record complaints and action requests and investigate ways to reduce resolution times (Recommendation 11).

WWC adopts a formalised process utilising the existing customer request system. Under this process, recording and actioning of complaints and requests has been improved and response times have significantly reduced. WWC also implemented a response target time of 14 days for complaints and service requests.

WWC partially implemented two recommendations:

- Document decisions to defer capital works and update subsequent renewal dates in the asset register (Recommendation 13).

  A 10-year works plan has been created which informs WWC's strategic asset management plan and long-term financial plan. However, the documentation is considered inadequate by WWC and further work is anticipated as part of council's strategic improvement plan. WWC has yet to fully implement this recommendation.

- Review the expenditure level on renewal and upgrade of its roads which considers the estimated lives of roads, because of their impact on sustainability ratios (Recommendation 14).

  A review of the useful-life of road surfaces and pavement assets has been completed, including analysis and the draft report has been independently peer reviewed. Remaining work includes re-drafting the report to address the feedback obtained via the peer review and submit to TAO for sign-off. WWC anticipates a significant increase to the useful lives of its roads. WWC is working towards implementation of this recommendation.

WWC has not implemented two recommendations:

- Monitor and document progress of its roads inspection program (Recommendation 12).
- Provide indicators of road condition and commentary on sustainability ratios in the annual report (Recommendation 15).

  WWC advised these recommendations had not been implemented due to resource constraints but remained future priorities in its strategic improvement plans.

  We accept WWC's position as delayed implemention of these recommendations does not create a serious risk.

4.4 Conclusion

CHC, DCC and NMC have either fully implemented or substantially implemented our recommendations.

WWC has fully or partially implemented the recommendations with the exception of two which it has delayed. These do not create a serious risk.

4.5 Submissions and comments received

Central Highlands Council

Central Highlands Council will include in the Financial Statements for 2017/18, explanatory commentary to the road condition and sustainability ratio information.

Lyn Eyles

General Manager

Devonport City Council

I advise that Council concurs with the findings in the 'Follow up of Auditor-General reports' relating to Devonport City Council and our progress of recommendations from the original report.

Paul West

General Manager

Northern Midlands Council

Council is satisfied with the report findings and have no further comments.

Your efforts in this matter are appreciated.

Des Jennings

General Manager

Waratah-Wynyard Council

Council accepts the findings and would like to reiterate that it is committed to completing the recommendations set out in the report from the 2015 audit.

Continued development of sound strategic asset management practices that are based upon the good governance principles of transparency, accountability and evidence-based decision making remains a key priority of this council to ensure sustainable and value-for-money service provision in the long term.

Shane Crawford

General Manager

LIST OF ACRONYMS AND ABBREVIATIONS

ASD	The Australian Signals Directorate (also known as the Defence Signals Directorate) is part of the Department of Defence.
Board	Board of Trustees
bn	Billion
CCTV	Closed circuit television
CHC	Central Highlands Council
DCC	Devonport City Council
DHHS	Department of Health and Human Services
DoE	Department of Education
DPAC	Department of Premier and Cabinet
DPEM	Department of Police and Emergency Management
DPFEM	Department of Police, Fire and Emergency Management
DPIPWE	Department of Primary Industries, Parks, Water and the Environment
eGovernment	The Office of eGovernment
Firewall	A system that controls incoming and outgoing traffic to the internet, establishing a barrier against threats to the network.
FTE	Full-time equivalent
ICT	Information and Communications Technology
Km	Kilometre
National Standards	National Standards for Australian Museums and Galleries, Version 1.3
NMC	Northern Midlands Council
School Viability Report	Ministerial Report — School Viability Reference Group Report to the Minister for Education and Skills
Server	A software program, or the computer on which that program runs, that provides a specific kind of service to client software running on the same computer or other computers on a network.
State Growth	Department of State Growth
STF	School Transition Fund
TMAG	Tasmanian Museum and Art Gallery
Treasury	Department of Treasury and Finance
Unauthorised media	Devices containing media, such as external hard drives, cameras, mobile phones, digital audio players and portable media players which have not been authorised for connection to government computer networks.
Whitelisting	Application whitelisting comprises the following technical steps: a. identifying specific programs and software libraries which should be permitted to execute on a given system b. preventing any other programs and software libraries from functioning on that system c. preventing users from being able to change which files can be executed.
WWC	Waratah-Wynyard Council

Page left blank intentionally

AUDIT MANDATE AND STANDARDS APPLIED

Mandate

Section 17(1) of the *Audit Act 2008* states that:

> 'An accountable authority other than the Auditor-General, as soon as possible and within 45 days after the end of each financial year, is to prepare and forward to the Auditor-General a copy of the financial statements for that financial year which are complete in all material respects.'

Under the provisions of section 18, the Auditor-General:

'(1) is to audit the financial statements and any other information submitted by a State entity or an audited subsidiary of a State entity under section 17(1).'

Under the provisions of section 19, the Auditor-General:

'(1) is to prepare and sign an opinion on an audit carried out under section 18(1) in accordance with requirements determined by the Australian Auditing and Assurance Standards

(2) is to provide the opinion prepared and signed under subsection (1), and any formal communication of audit findings that is required to be prepared in accordance with the Australian Auditing and Assurance Standards, to the State entity's appropriate Minister and provide a copy to the relevant accountable authority.'

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.

Tasmanian
Audit Office

Phone	(03) 6173 0900	**Address**	Level 8, 144 Macquarie Street, Hobart
Fax	(03) 6173 0999		
email	admin@audit.tas.gov.au	**Postal Address**	GPO Box 851, Hobart 7001
Web	www.audit.tas.gov.au	**Office Hours**	9am to 5pm Monday to Friday

Launceston Office

Phone	(03) 6173 0971	**Address**	2nd Floor, Henty House 1 Civic Square, Launceston