Tasmanian
Audit Office

Report of the Auditor-General No. 8 of 2014-15

Security of information and communications technology (ICT) infrastructure

March 2015

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.

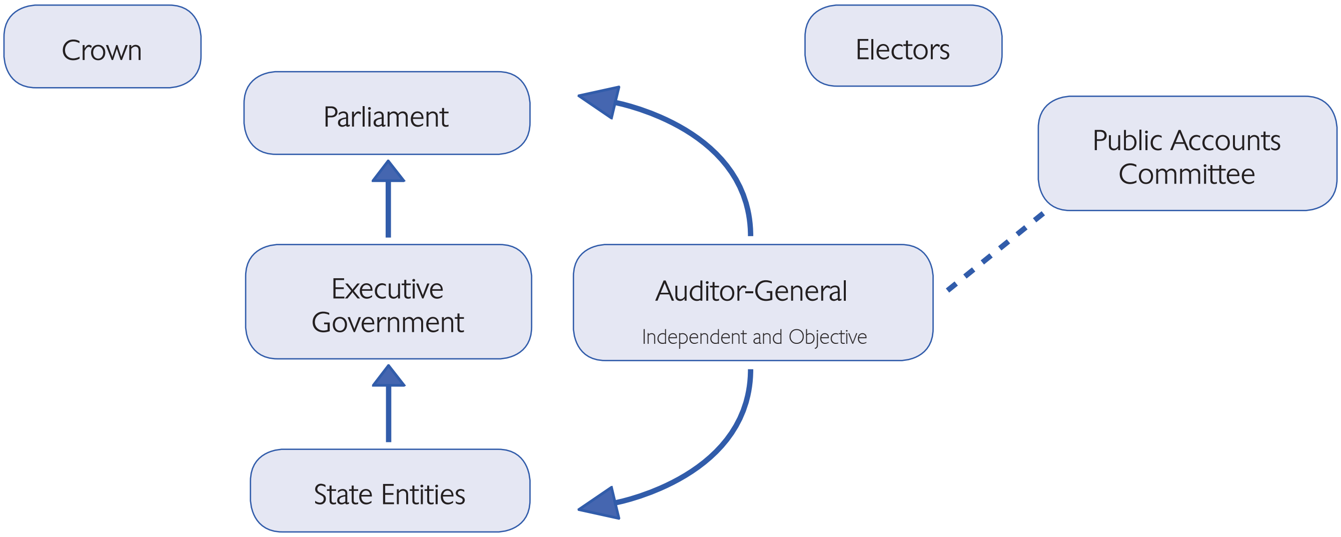
We can also carry out investigations but only relating to public money or to public property. In addition, the Auditor-General is now responsible for state service employer investigations.

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.



2015 No. 3

2015

PARLIAMENT OF TASMANIA

REPORT OF THE AUDITOR-GENERAL No. 8 of 2014–15

Security of information and communications technology (ICT) infrastructure

March 2015

Presented to both Houses of Parliament in accordance with the provisions of the Audit Act 2008

This report, and other Auditor-General Reports, can be accessed via our home page (http://www.audit.tas.gov.au).

For further information please contact:

Tasmanian Audit Office

GPO Box 851

Hobart

TASMANIA 7001

Phone: (03) 6226 0100, Fax (03) 6226 0199

Email: admin@audit.tas.gov.au

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

ISBN: 978-0-9925757-3-1

Tasmanian
Audit Office

Level 4, Executive Building, 15 Murray Street, Hobart, Tasmania, 7000
Postal Address GPO Box 851, Hobart, Tasmania, 7001
Phone: 03 6226 0100 | Fax: 03 6226 0199
Email: admin@audit.tas.gov.au
Web: www.audit.tas.gov.au

26 March 2015

President
Legislative Council
HOBART

Speaker
House of Assembly
HOBART

Dear Mr President
Dear Madam Speaker

REPORT OF THE AUDITOR-GENERAL
No. 8 of 2014–15: ***Security of information and communications technology (ICT) infrastructure***

This report has been prepared consequent to examinations conducted under section 23 of the *Audit Act 2008.* The objective of the audit was to assess the effectiveness of security measures for ICT infrastructure at five government departments.

Yours sincerely

H M Blake
AUDITOR-GENERAL

This page left blank intentionally

Contents

List of tables

Foreword

State entities operate in an increasingly complex environment, no more so than in the area of information and communications technology where there is a constant need to be abreast of increasingly rapid change. This situation was a factor in our decision to benchmark the performance of five government departments against a high threshold, that is, prioritised strategies listed by the Australian Signals Directorate. Our approach was supported by the five departments at audit commencement.

My audit acknowledged from the outset that a whole of government project was underway to produce an ICT Security Framework, including a Government ICT Security Manual. This initiative is supported. I encourage its early completion and that the manual address recommendations made in this audit. I also encourage the Department of Premier and Cabinet initiate a review of the Framework at a suitable date post implementation.

As a result of the high number of weaknesses identified, I concluded that there were areas of inadequate security at most departments. Common problems included lack of policy on physical security, construction weaknesses, limited CCTV coverage, excessive risk from cyber-attacks and lack of testing of backups. I am also concerned at the lack of a strategic approach to ICT security. Hopefully the ICT Security Framework referred to will address these matters.

However, this is not to say that the departments audited are not taking ICT security seriously. Evident from this report, and from submissions made by Secretaries, is that, generally, departments had reasonable security over most of their facilities, infrastructure and servers and I, and the community, should be confident that data is, or that steps are being taken to ensure, appropriately secure.

My normal practice when finalising reports is to provide those charged with governance, in this case the five Secretaries, approximately two weeks to provide formal responses to my reports and then to table at the earliest opportunity. This ensures timely reporting to the Parliament post audit completion and would, in the normal course of events, have resulted in a public report in late December 2014 or early January 2015. On this occasion, however, I decided not to table this report at the earliest available opportunity. To do so may have exposed government departments' vulnerabilities to malicious activity. To allow departments some time to strengthen security of their ICT assets, the response time was extended by three-months. As indicated from responses provided. Departments have used this time well.

H M Blake

Auditor-General

26 March 2015

List of acronyms, abbreviations and key definitions

ASD	The Australian Signals Directorate (also known as the Defence Signals Directorate) is part of the Department of Defence.
CCTV	Closed Circuit Television
DHHS	Department of Health and Human Services
DMZ	DMZ or 'demilitarized zone' is a group of computers placed between the network and the internet to provide a further layer of protection to that network from threats coming from the internet.
DPaC	Department of Premier and Cabinet
DPEM	Department of Police and Emergency Management
DPIPWE	Department of Primary Industries, Parks, Water and the Environment
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
Network infrastructure	Our use of this term covers in-building cabling (i.e. backbone cabling), switches, routers and data communications equipment.
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.
SOE	Standard Operating Environment (a consistent, enforced configuration and set of applications for every workstation).
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.

Executive summary

Executive summary

Background

Government departments rely on information and communications technology (ICT) which supports key systems such as patient management, police operations and motor registry. ICT infrastructure and data needs protection from equipment failure, data loss or cyber-attack[1].

An illustration of the need for effective protection was an outage of Hobart's Bathurst Street data centre early in January 2012. An equipment fire caused a two to three day shutdown of various government servers and communications hardware.

Traditionally, Government's approach to ICT security has been agency-based with some whole-of-government support for management and planning. While this model has suited government well in the past, a more coordinated and strategic focus has become necessary due to the expanded range of online government services and increasingly sophisticated threats to security.

Part of the audit involved a review of cyber security that was based on prioritised strategies listed by the Australian Signals Directorate (ASD)[2]. At least 85 per cent of intrusions that ASD responded to in 2011 involved unsophisticated techniques that would have been mitigated by the 'Top 4' mitigation strategies.[3]

At the time of the audit, a whole-of-government project, sponsored by DPAC, was under way to produce an ICT Security Framework. The project's terms of reference included producing a Government ICT Security Manual. The work was not sufficiently advanced to be considered in the audit and our testing was done at an individual department level.

Audit objective

The objective of the audit was to assess the effectiveness of security measures for ICT infrastructure in government departments.

[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.

[3] For more detail see page 31.

Audit scope

The audit included ICT physical infrastructure, applications and information. Departments subject to audit were:

- Treasury and Finance (Treasury)
- Primary Industries, Parks, Water and Environment (DPIPWE)
- Health and Human Services (DHHS)
- Premier and Cabinet (DPAC)
- Police and Emergency Management (DPEM).

Detailed audit conclusions

The following audit conclusions are based on criteria we applied to each of the five departments in scope. The following sections and their tabulated ratings are aligned to the sections and subsections in Chapters 1–5 that cover each department. Detailed rationales underlining the ratings assigned are provided in corresponding sections of the Report.

In a departure from our usual practice, we decided to not table this report at the earliest available opportunity. To do so may have exposed government departments' vulnerabilities to malicious activity. To allow departments some time to strengthen security of their ICT assets, we extended the management response period by three-months.

Was there physical security over facilities, network infrastructure and servers, within government buildings?

Table 1 shows our assessments against individual elements of physical security.

Table 1: Physical security — summary*

Department	Treasury	DPIPWE	DHHS	DPAC	DPEM
Access to server rooms and servers	P	P	P	P	✓
Protected network infra-structure	✓	P	✗	✗	P
Physical facilities certified or accredited	Currently there is no accreditation process available				

* The ratings used in Tables 1–8 are: ✓ = pass; ✗ = fail; P = partial.

Generally, departments had reasonable security over most of their facilities, infrastructure and servers. However, there were areas of inadequate security at most departments. Common problems included lack of policy on physical security, construction weaknesses and limited CCTV coverage.

Was information safe and secure?

Table 2 shows our assessments against individual elements of information security.

Table 2: Information security — summary

Department	Treasury	DPIPWE	DHHS	DPAC	DPEM
Effective data back up	✓	✓	P	P	✓
Data safe from cyber-attack	P	✗	✗	✗	✗
Restricted data access	✓	✓	✗	✓	✓

Information was generally safe and secure with reasonable backup and access restrictions. However, all departments 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 backups and access permissions.

Was there a strategic approach to ICT security?

Table 3 shows our assessments of strategic approaches taken to ICT security.

Table 3: Strategic approach to security — summary

Department	Treasury	DPIPWE	DHHS	DPAC	DPEM
ICT security plan	✗	✗	✗	✗	✓
ICT security governance committee	✓	✓	✓	✓	✓
Inbuilt security controls	P	✓	✓	P	P
Incident recording	✓	✗	✗	✗	✗
BCP and DRP*	✓	✗	✗	P	✗

* BCP = business continuity plan. DRP = disaster recovery plan.

There was widespread failure of departments to take a strategic approach to ICT security evidenced by lack of ICT security plans, incident recording systems as well as business continuity and disaster recovery plans.

Recommendations made[4]

The Report contains the following recommendations:

Rec	Section	Dep't	We recommend that ...
5	1.3.2	All departments	fully implement at least the 'Top 4' mitigation strategies from *Strategies to Mitigate Targeted Cyber Intrusion*.
1	1.2.1	Treasury	includes physical security of servers and server rooms in its ICT security policy. We also recommend that Treasury considers use of CCTV monitoring.
3	1.3.1		tests backups at a frequency commensurate with risk.
4	1.3.2		disables local administrator accounts.
6	1.3.3		reviews monitoring of system access by business units audit access to ensure consistency across all systems.
7	1.4.1		develops a specific ICT security plan and updates its ICT security risk review.
8	1.4.3		makes greater use of inbuilt IT controls such as enforcing password standards and controls over use of unauthorised media.
9	1.4.5		conducts a full disaster recovery test.
10	2.2.1	DPIPWE	updates its ICT security policy and upgrades access controls, alarms and hazard protection at specific server rooms where necessary.
11	2.2.2		provides protective covering for any exposed building cabling and provides basic security of switches and routers.
12	2.3.1		uses off-site storage for all backup tapes. Backup procedures should be recorded and testing logs maintained.
13	2.3.2		considers the use of firewalls for workstations throughout the department and also disables local administrator accounts.

[4] At the time of the audit, a whole-of-government project was under way to produce an ICT security framework. Some of our recommendations — while at the departmental level — could potentially be overtaken by implementation of the whole-of-government project.

Rec	Section	Dep't	We recommend that …
14	2.3.3		develops a policy to ensure that access to confidential information is valid and that no unused accounts exist. DPIPWE should also implement regular testing and monitoring of user access.
15	2.4.1		implements an ICT security plan and associated risk management plan.
16	2.4.3		implements inbuilt control over use of unauthorised media.
17	2.4.4		implements an ICT security incident recording and management system.
18	2.4.5		develops business continuity plans and ICT security disaster recovery plans and tests plans regularly.
19	3.2.1	DHHS	upgrades access controls, alarms and hazard protection at specific server rooms where necessary.
20	3.2.2		sets standards for physical security and implements specific protections accordingly.
21	3.3.1		tests backups at a frequency commensurate with risk.
22	3.3.2		○ implements application-based workstation firewalls ○ implements multi-factor authentication for external access ○ addresses its consultant's concern that the network was poorly segmented.
23	3.3.3		○ develops a policy to ensure that access to confidential information is valid and that no unused accounts exist that can be wrongfully used ○ audits access privileges to bring accounts up to date ○ implements regular testing and monitoring of user access.
24	3.4.1		implements an ICT security plan and associated risk management plan.

Rec	Section	Dep't	We recommend that …
25	3.4.3		makes greater use of inbuilt IT controls such as enforcing password standards and controls over use of unauthorised media.
26	3.4.4		rationalises its incident management system and develops a means of specifically recording and analysing ICT security incidents and near misses.
27	3.4.5		while DHHS implements its dual data centre approach, the department should produce business continuity and disaster recovery plans and test them regularly.
2	1.2.3	DPAC	outlines requirements for varying levels of security and develops guidelines to allow departments to self-assess and accredits those departments' various security zones.
28	4.2.1		upgrades its coverage of physical security in its ICT security policy. We also recommend that DPAC reviews construction of server rooms, expanded use of CCTV and greater hazard protection.
29	4.2.2		sets standards for physical security and implements specific protections accordingly.
30	4.3.1		tests backups and retains test documentation to provide assurance that restores will function correctly.
31	4.3.2		disables local administrator accounts.
32	4.3.3		enforces its password parameters in line with departmental policy.
33	4.4.1		develops a specific ICT security plan.
34	4.4.3		makes greater use of inbuilt IT features such as time-outs on personal computers, enforcing password standards, controls over unauthorised media and software.
35	4.4.4		modifies its help desk system to enable it to record security near misses.

Rec	Section	Dep't	We recommend that …
36	4.4.5		improves its disaster recovery plan by identifying responsible officers, linking to risk management documentation, covering security breaches and cyber-attacks as well as setting recovery time objectives. We further recommend that the department documents tests of its disaster recovery plan.
37	5.2.2	DPEM	sets standards for physical security and implements specific protections accordingly.
38	5.3.1		documents its backup and restore procedures.
39	5.3.2		○ disables local administrator accounts ○ implements application-based firewalls.
40	5.3.3		fully documents its access procedures and implements a regular program of access testing.
41	5.4.1		specifies in its ICT security plan that risk reviews should take place regularly.
42	5.4.3		makes greater use of inbuilt IT controls such as controls over unauthorised software, media and internet access.
43	5.4.4		implements an IT security incident management and recording system.
44	5.4.5		formalises, implements and tests business continuity and disaster recovery plans.

This page left blank intentionally

Audit Act 2008 section 30 — Submissions and comments received

Audit Act 2008 section 30 — Submissions and comments received

Introduction

In accordance with section 30(2) of the *Audit Act 2008*, a copy of this Report was provided to the state entities indicated in the Introduction to this Report.

A summary of findings, with a request for submissions or comments, was also provided to the relevant portfolio ministers and the Treasurer.

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

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

Department of Treasury and Finance

Thank you for your letter of 16 December 2014 and the attached draft Report to Parliament for the above performance audit.

Treasury's management responses are included below:

Recommendation 1

Treasury will include physical security of servers and server rooms in its ICT security policy. Access to Treasury buildings is tightly controlled with swipe card access and CCTV monitoring is in place both internally and externally in many areas. We do not believe that on a cost/benefit basis installation of further CCTV monitoring is warranted.

Recommendation 2

To be addressed by DPAC.

Recommendation 3

As noted in the report, Treasury has an effective and reliable back-up system and a risk based approach is used in testing the system.

Recommendation 4

Treasury only has a single local administrator account that is only able to be accessed by a few selected IT system administrators. End users do not know this account and cannot access their PCs as local administrators. Without this account significant IT staff time and effort and end-user staff disruption would result when an issue arises where a PC cannot authenticate against the domain. Treasury has strong security management practices in-place for this local account and therefore consider the benefits for this account outweigh the risks.

Recommendation 5

The only other mitigation strategy from the ASD, apart from the administrator access issue mentioned above, which Treasury does not have in place is application whitelisting. As noted in the report this provides for software control over malicious programs from any source. The controls currently in-place at Treasury include:

- Only selected IT staff have the required access to install software on Treasury computers;
- ISB staff will only install approved software on Treasury computers;
- Only Treasury devices (PCs, laptops, etc.) can connect to the Treasury Domain and all Treasury devices are regularly patched for security and run anti-virus and anti-malware software.

Following a risk assessment of this issue and on a cost/benefit basis, Treasury is comfortable with the current strategy.

Recommendation 6

Accepted. Treasury will review the monitoring of systems access by business units to ensure consistency.

Recommendation 7

Treasury has a comprehensive suite of ICT security policies, standards and guidelines and an incident reporting system. We will investigate the need for an ICT Security Plan if there are any gaps in our documentation and processes.

High level ICT Security risks were reviewed as part of the annual review of Treasury's strategic risks which was completed by the Executive in late 2014. We have also scheduled a review of Information Management and ICT risks for Q1 2015.

Recommendation 8

Treasury has considered this issue and considers the benefits of the current policies outweigh the risks.

Recommendation 9

Treasury's policy is to undertake disaster recovery and business continuity plan testing on an on-going basis. This is done each time a system or component of a system infrastructure is upgraded or replaced. Treasury has also conducted risk assessments to consider the need for full Disaster Recovery testing and has made a risk based decision that this has not been needed since the full Disaster Recovery test performed late in 2011. Treasury has full redundancy capability in-place between its major sites in the Hobart CBD.

Tony Ferrall
Secretary

Department of Primary Industries, Parks, Water and Environment

Our Department agrees that a coordinated and strategic focus in managing ICT security is important, and I believe that the work being undertaken at a whole of Government level under the auspices of the ICT Policy Board will achieve this. In that context, I note that the scope of the audit did not appear to include a number of projects currently underway across Government that will align ICT infrastructure and standards, such as the assessment of data centres and the development of the ICT security framework as part of the Networking Tasmania 2 (NTIII) tender.

Our department's main concern with the premise of the Draft Report, and this has been discussed with officers in your Office, is the assessment of the Department against the Australian Signals Directorate (ASD) ICT security standards. These standards are the "gold standard" for the Australian Defence Force and do not align with the Tasmanian Government's own Information Security Manual, the implementation of which DPIPWE have been working towards.

The Government's Information Security Policy is now being reviewed by the ICT Policy Board as elements of the Manual did not consider the level of risk appropriate to Agencies. The ICT Policy Board has noted that there needs to be further consideration of the resource costs associated with implementation and that these need to be assessed against the minor levels of risk associated with the information being secured.

Whilst ASD publications are being used as a guide in these processes, as there are major differences in the level of risk and business functions and operations of Australian Government and Tasmanian Government agencies, we should be prudent in adopting only those elements of the ASD that are suited to our risk profile and business functions, rather than attempting a "one size fits all". Applying the ASD standard would potentially increase the cost of implementation and administration of ICT with little or no benefit comparable with the associated risk.

It is agreed that there needs to be a more consistent approach across Government for ICT security. This is being driven by the increase in sharing of ICT resources, which is increasing the level of shared risk, as well as the benefits in sharing expertise across Government.

With respect to the specific recommendations relevant to DPIPWE:

TAO Recommendation 1

ASD Recommendation l

DPIPWE currently do not have any form of application whitelisting, however will investigate the options available and make a recommendation to the DPIPWE Information Management Sub Committee as to the best approach.

The investigation will consider the implementation on a risk based approach for the Agency, costs to administer; and education of staff required.

ASD Recommendation 2

DPIPWE currently patch mainline and high risk applications such as Microsoft, Adobe software, ArcGIS, Google Earth, MapInfo etc. The Agency will continue to perform such patching in a timely manner with the versions of software and applied patches identifiable in DPIPWE's System Centre Configuration Manager (SCCM).

ASD Recommendation 3

As with ASD Recommendation 2, vendor operating system patches are installed through SCCM after testing on a QA group to ensure no adverse impact to clients are identified. For extreme risk vulnerabilities these are treated with high priority and deployed as soon as possible.

ASD Recommendation 4

No administrator privileges are granted by default in DPIPWE. Group policy is used to allow administrative rights to work stations. The Agency will review the current group policies, and based on risk analysis to the Agency, make any necessary amendments to current group policies.

Recommendation 10

DPIPWE will review its ICT security policy including a review of the current access controls and hazard protection to the main server rooms. This will be risk based and take into consideration the cost of the upgrades and whole of Government direction of moving to third party data centres by 2018.

Recommendation 11

DPIPWE will review the protective coverings for any exposed building cabling to its main server rooms. This will be risk based and take into consideration the cost of the works required and whole of Government direction of moving to third party data centres by 2018

Recommendation 12

As advised during the audit, DPIPWE has reviewed it backup procedures and is now storing all backup tapes off site and maintaining testing logs. Backup procedures are now formally documented.

Recommendation 13

Where the set of applications used is fixed (e.g. Service Tasmania) firewalls are enabled at the workstation. To enable line of business applications blocked by a workstation firewall local administrator privileges are needed, or group policies need to be amended by ICT support.

DPIPWE will investigate the impact of enabling workstation firewalls and based on the impact to productivity, impact on the removal of local administration privileges (ASD Recommendation 4 and also Recommendation 14) and additional workload will revise the current deployment of workstation firewalls.

No local administrator accounts are granted by default in DPIPWE. Group policy is used to allow administrative rights to work stations. DPIPWE will review the current group policies and, based on risk analysis to the Agency, alter current group policies.

Recommendation 14

While DPIPWE currently has no formal policy, in practise automated processes disable inactive accounts and they are also manually disabled on receipt of the regular staff movement notices from HR.

Once confidential information has been fully identified by business units, in order to implement the Information Security Manual, DPIPWE will investigate automating reports and tools to aid the business units in testing and monitoring levels of user access to data including confidential information.

Recommendation 15

DPIPWE are involved in the ICT security review as part of the Networking Tasmania III project. This will ensure all agencies are implementing security uniformly across Government based on the appropriate risk identified for the work area involved. Once this plan is completed it will serve closely as the basis for DPIPWE's ICT security and associated risk management plan.

Recommendation 16

There are many complexities around the implementation of inbuilt controls over unauthorised media that necessitate a detailed investigation as to the business impact of this recommendation. DPIPWE will investigate the impact, consult with other departments on their strategies, and, consider the implementation of these controls.

Recommendation 17

DPIPWE are now using their incident management system to clearly tag any ICT security incident that is raised or reported. Reports can be generated listing all the ICT security incidents reported.

Recommendation 18

This will be undertaken in conjunction with the development of the Agency business continuity plan.

John Whittington
Secretary

Department of Health and Human Services

Thank you for the opportunity to comment formally on your recent performance audit report: Security of ICT Infrastructure.

The Department of Health and Human Services' response to Recommendations 19-27 of the report are detailed as follows:

Recommendation 19

Agree in principle. Implementation is on hold pending resolution of Recommendation 20 and clarification from DPAC on Whole of Government Standards for physical security of server rooms.

Recommendation 20

Agree in principle. Implementation is on hold pending clarification from DPAC on Whole of Government requirements as per Recommendation 2.

Recommendation 21

Agreed. Backups are regularly tested and further discussions with internal Business Groups and System Owners regarding appropriate risk assessments, test plans and supporting Service Level Agreements are expected to address this recommendation.

Recommendation 22

a) Agree in principle, however there are many applications in use throughout the Department of Health and Human Services (DHHS) and the impacts of this in terms of time and costs could be high. The architecture of particular applications may need to be extensively modified to accommodate this approach. Further analysis is therefore necessary to determine the associated costs, risks, and clinical usability associated with the implementation of application-based workstation firewalls.

b) Agreed. The DHHS is currently trialling the use of multi-factor authentication for external access, and expects to have this in place before Quarter 3 of 2015.

c) Agreed in principle. Further analysis is necessary to determine the associated costs, risks, and clinical usability associated with the segmentation.

Recommendation 23

Agreed in principle. Further analysis is necessary to determine the associated costs, risks, and clinical useability.

Recommendation 24

Agreed. The DHHS is currently updating its Risk Management Plan in preparation for the development of appropriate ICT Security Plans.

Recommendation 25

Agreed in principle. Further analysis is necessary to determine the associated costs, risks, and clinical useability.

Recommendation 26

Agreed. Implementation is underway. The DHHS now records and analyses ICT security incidents and near misses.

Recommendation 27

Agreed. This activity is included in Phase 3 of the Infrastructure Stabilisation Project.

Michael Pervan
Acting Secretary

Department of Premier and Cabinet

Thank you for your letter of 16 December 2014 providing the opportunity to comment on your performance audit report to Parliament on the Security of ICT Infrastructure.

I agree with the view expressed in the introduction of the report that we need a more coordinated and strategic focus to manage ICT security. Consistent with that, I would like to draw to your attention to a number of current approaches at a whole-of-government level to ICT security.

The Tasmanian Government Information Security Policy, and its supporting Manual, contains procedures and advice specific to the scope of your audit, namely risk management, physical environment, incident management and business continuity management. Specific ICT security advice also forms part of this Manual.

The Manual also makes reference to the Tasmanian Government WAN and Internet Services Information Security Policies and Standards which documents information security requirements relating to the Networking Tasmania II (NT II) agreements.

Implementation of the Tasmanian Government WAN and Internet Services Information Security Policies and Standards security measures (including proactive monitoring, management, reporting and audits) that sit around agency ICT infrastructure is provided and managed through the NT II agreements which are managed by TMD within my Department. The NT ll agreements include services provided by contractors such as Telstra. As part of the agreements, TMD and key contractors have relationships with organisations such as the Australian Signals Directorate.

Recognising that our approach to ICT Security needs updating, the ICT Policy Board is currently developing a contemporary whole-of-government ICT Security Framework. This new Framework will provide a consistent, risk based and systems approach to ICT security and will replace existing whole-of-government ICT security policies and guidance. I note that this new Framework was not assessed as part your audit as it is still under development. I anticipate this work will be completed in the third quarter of 2015 and I will forward the work to you once it has been endorsed by the ICT Policy Board.

To address shortcomings in the quality of agency owned data centres the Tasmanian Government is working on a strategy to close existing government owned and operated data centres and move to the 'Tasmanian Cloud'. The initial elements of this strategy, whole-of-government contracts for data centre services, are already in place through the NT II agreements.

The DPAC specific ICT security issues identified in your report are noted and are being appropriately addressed by DPAC. This includes reviewing operational procedures and planning the process to migrate out of DPAC operated data centres to facilities available through the NT II agreements.

Thank you again for providing the opportunity to comment on your report.

Greg Johannes
Secretary

Department of Police and Emergency Management

The responses to the recommendations of your security audit of DPEM's ICT infrastructure are below.

Recommendation 37

DPEM accepts the recommendation. The policy and controls for physical security is currently awaiting approval and an implementation plan is currently underway.

Recommendation 38

DPEM accepts the recommendation and the required documentation has been completed.

Recommendation 5

1. Application whitelisting: DPEM has implemented application whitelisting.

2. Patching applications: DPEM has written the procedures for implementing patches on applications in response to recommendations from the vendor and has introduced a mechanism for documenting the patching of applications.

3. Patching operating system: DPEM has changed its procedures for patching operating systems to being in response to recommendations from the vendor.

4. Minimise administrative privileges: DPEM already complies with this strategy.

Recommendation 39

DPEM accepts the recommendation and has disabled workstation local administrator accounts and implemented application-based workstation firewalls.

Recommendation 40

DPEM accepts the recommendation. The policy and controls for information systems access control is currently awaiting approval. A regular testing program will be implemented.

Recommendation 41

DPEM accepts the recommendation. The ICT security plan has been updated to include a regular review of risks and is currently awaiting approval.

Recommendation 42

DPEM accepts the recommendation. Inbuilt controls have been implemented to control internet access and the use of unauthorised software.

The Department will review the appropriateness of the duration for timed lockouts based on operational requirements.

Inbuilt controls over unauthorised media are currently being investigated and will be implemented on a risk versus operational requirement.

Recommendation 43

DPEM accepts the recommendation. An IT security incident management and recording system has been implemented.

Recommendation 44

DPEM accepts the recommendation. Business continuity and disaster recovery plans have been completed and a regular testing regime implemented.

Darren Hine
Secretary

Introduction

Introduction

Background

Government businesses rely on information and communications technology (ICT) which supports key systems such as patient management, police operations and motor registry. ICT infrastructure and data needs protection from equipment failure, data loss or cyber-attack[5].

An illustration of the need for effective protection was an outage of Hobart's Bathurst Street data centre early in January 2012. An equipment fire caused a two to three day shutdown of various government servers and communications hardware.

Traditionally, government's approach to ICT security has been agency-based with some whole-of-government support for management and planning. While this model has suited government well in the past, a more coordinated and strategic focus has become necessary due to the expanded range of online Government services and increasingly sophisticated threats to security.

At the time of the audit, a whole-of-government project, sponsored by DPAC, was under way to produce an ICT security framework. The project's terms of reference included producing a government ICT security manual. The work was not sufficiently advanced to be considered in the audit and our testing was done at an individual department level.

Audit objective

The objective of the audit was to assess the effectiveness of security measures for ICT infrastructure in government departments.

Audit scope

The audit included ICT physical infrastructure, applications and information. Departments subject to audit were:

- Treasury and Finance (Treasury)
- Primary Industries, Parks, Water and Environment (DPIPWE)

[5] 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.

- Health and Human Services (DHHS)
- Premier and Cabinet (DPAC)
- Police and Emergency Management (DPEM).

Audit criteria

The audit criteria were:

- adequacy of physical security over facilities, network infrastructure and servers in government buildings
- safety and security of information
- existence of a strategic approach to ICT security.

In this Report, each criterion is assessed on a chapter-by-chapter basis for each of the departments mentioned above.

Audit approach

The audit involved:

- questionnaires completed by audit clients
- review of policies and other documentation
- site visits
- testing
- interviews.

We did not undertake penetration testing of cyber security. We considered that no system was foolproof and that using an expert to breach security would not necessarily demonstrate poor security. Instead, our review of cyber security was based on prioritised strategies listed by the Australian Signals Directorate (ASD)[6]. At least 85 per cent of intrusions that ASD responded to in 2011 involved unsophisticated techniques that would have been mitigated by the 'Top 4' mitigation strategies[7]. In our audit testing, we applied ten mitigation strategies with emphasis on the Top 4.

The audit also used benchmarks from the:

- Australian Information Commission
- Australian Government Information Security Manual[8]

[6], ASD, *Strategies to Mitigate Targeted Cyber Intrusions*., October 2012

[7] For more detail see page 31.

[8] The Guide contains a section on ICT Security measures. ASD produces the *Information Security Manual* that contains controls for ICT security.

- *Tasmanian Government Identity and Access Management Toolkit*[9]
- *Australian Government Physical Security Management Protocol.*

Timing

Audit planning began in August 2013. Fieldwork was completed in August 2014 and the report was finalised in November 2014.

Resources

The audit plan recommended 900 hours and a budget, excluding production costs, of $151782. Total hours were 1224 and actual costs, excluding production, were $186 486, which exceeded our budget.

Why we did this audit

This audit was undertaken because the subject area is a matter of ongoing public interest and has experienced significant change in recent years. Our commitment to this audit topic was publicly disclosed in the *Annual Plan of Work 2013–14*, available on our website.

[9] Published by the Office of eGovernment in the Department of Premier and Cabinet.

1 Department of Treasury and Finance

1 Department of Treasury and Finance

1.1 Introduction

In 2013–14, Treasury's annual budget was $49m and the department had 284 full time equivalent staff (FTEs). Treasury had responsibility for management of the State budget, State-based tax collection and in 2013–14 administered revenue from Government businesses of $417m in the form of dividend payments, tax equivalents and guarantee fees.

ICT systems played a major role in enabling Treasury to perform its role and we expected:

- effective physical security over facilities, network infrastructure and servers within Treasury buildings (Section 1.2)
- that information kept on ICT systems at Treasury was safe and secure (Section 1.3)
- a strategic approach to ICT security. (Section 1.4)

As a central government department, Treasury had the advantage of being comparatively self-contained. On the other hand, Treasury could be viewed as a target for hackers due to the importance of its role.

1.2 Was there physical security over facilities, network infrastructure and servers, within government buildings?

In order to assess the effectiveness of physical security to protect server rooms, network infrastructure and other hardware in Treasury buildings, we examined whether there was:

- effective physical security over server rooms and servers (Section 1.2.1)
- effective physical security over network infrastructure (Section 1.2.2)
- any certification or accreditation regime for ICT physical security. (Section 1.2.3)

Tasmanian government entities are required to comply with the *Tasmanian Government Identity and Access Management Toolkit*. We also checked compliance with the *Australian Government Physical Security Management Protocol.*

1.2.1 *Was there effective physical security over the server room and servers?*

We examined whether server rooms and servers had effective alarms, access controls (including control over third parties), intruder detection and hazard protection (fire, flood or power problems) to provide reasonable security over damage to equipment and unauthorised systems access.

Treasury's ICT security policy did not explicitly cover physical security. Nonetheless, we found that reasonable controls existed over server rooms and servers. Greater security could be achieved by:

- more robust construction of server rooms — to overcome inherent weaknesses such as suspended ceiling and stud walls[10]
- improved use of CCTV.

Recommendation 1

We recommend that Treasury includes physical security of servers and server rooms in its ICT security policy. We also recommend that Treasury considers use of CCTV monitoring.

1.2.2 *Was there was effective physical security over network infrastructure?*

We expected that there would be control measures to protect network infrastructure such as building cabling and routers. In our view, these items need to be out of sight and secured by basic level locks and keys in order to prevent accidental or malicious damage.

We noted that network infrastructure was protected by building security and was in access-controlled areas. Routers and switches were housed in locked cupboards.

Building cabling had been installed by licensed contractors working to Australian standards. Frequently, cabling within buildings was run in riser shafts secured by keyed locks.

We concluded that adequate security measures had been taken to protect network infrastructure.

[10] Suspended ceilings allow a crawl space that could offer intruder access from another room.

1.2.3 Were physical facilities certified and accredited?

The *Australian Government Physical Security Management Protocol* calls for hierarchical security zoning and accreditation for measures taken for each zone.

At the commonwealth level, we noted that agencies were required to apply control measures from applicable security guidelines. Agencies are then to certify application of the measures and accredit the security zones in line with the protocol. No equivalent process existed at the Tasmanian level.

Treasury had achieved a zoned approach in the sense that swipe card access applied to general office areas, with additional security for ICT facilities. However, the approach was not formally documented and was not based on formal requirements or guidelines.

Recommendation 2

We recommend that DPAC outlines requirements for varying levels of security and develops guidelines to allow departments to self-assess and accredits those departments' various security zones.

1.3 Was information safe and secure?

Government departments have to protect information. To determine whether they have, we applied the following criteria to ascertain whether data was:

- backed up effectively (Section 1.3.1)
- safe from cyber-attack (Section 1.3.2)
- accessible only to appropriate staff. (Section 1.3.3)

1.3.1 Was data backed up effectively?

We expected an effective backup process to:

- be fully documented
- have backup logs
- have safe and appropriate storage with backup tapes stored at a separate location
- test backups regularly.

We found that Treasury used a proprietary software system that documented each backup. The system provided indications of failed files in backups.

We were satisfied that there was:

- reliable backup

- adequate documentation
- offsite storage of tapes.

Treasury explained that requests from staff for files to be restored were sufficiently frequent to provide assurance that backups were reliable. However, we believed a routine test process can provide much greater certainty that all data can be restored than ad hoc requests. Accordingly, we concluded that backups were not systematically tested.

Recommendation 3

We recommend that Treasury tests backups at a frequency commensurate with risk.

1.3.2 Was data safe from cyber-attack?

As mentioned in the Introduction, we tested against ten mitigation strategies from *Strategies to Mitigate Targeted Cyber Intrusions*[11]. Table 4 shows the strategies in number order and our assessments against them. The 'Top 4' are at the head of the Table and are considered by ASD to be essential.

[11] ASD, *Strategies to Mitigate Targeted Cyber Intrusions.*, October 2012

Table 4: Mitigation strategies at Treasury

Strategy	Rating
Application whitelisting (listing of trusted programs, not allowing installation of non-trusted software). This is the top strategy because it provides control over malicious programs from any source including emails, USBs and the internet.	✗[1]
Patching applications (monitoring for patches for 'extreme risk' vulnerabilities, timely installation, list software and patches applied)	✓
Patching operating system (monitoring for patches for 'extreme risk' vulnerabilities, timely installation, maintain history of patches applied).	✓
Minimising users with administrative privileges	✓
Disabling local administrator accounts (involves more than password control)	✗[2]
Application-based workstation firewall	✓
Multi-factor authentication (e.g. use of a token and a password)	✓
Network segmentation (partitioning the network) and segregation (rule-based) into security zones to protect sensitive information and critical services	✓
Host-based intrusion detection/prevention system	✓
Centralised and time-synchronised logging	✓

[1] Not performed, although Information Systems Branch staff install non-standard software as approved by the Director ISB.

[2] Local administrator accounts, unique to each computer, were not disabled, although password control existed.

Treasury had implemented most of the selected risk mitigation strategies. The network was effectively segmented, and some mitigation strategies were carried out on a whole-of-government contract. We tested whether the users with administrative privileges were appropriate and only current staff had accounts.

In our assessment, Treasury data was at medium risk from cyber-attack. Despite the mitigation strategies in place, security could be improved by implementing application whitelisting and by disabling local administration accounts.

Recommendation 4

We recommend that Treasury disables local administrator accounts.

Recommendation 5

We recommend that all departments fully implement at least the 'Top 4' mitigation strategies from the Australian Signals Directorate publication: *Strategies to Mitigate Targeted Cyber Intrusions*.

1.3.3 Was data access only available to appropriate staff?

We tested for:

- policies and procedures that ensured:
  - staff access to data was limited to a need-to-know basis
  - no superfluous accounts were maintained (in light of staff movements, new starts, transfers and terminations)
- testing, monitoring and logging of access.

We tested a selection of users for several applications and verified that each had appropriate, properly authorised access. Testing was also performed on new starts, staff movements and terminations, verifying that the process for updating access was performed accurately and that the notifications were sent at appropriate times.

Treasury policy specified that access controls should be monitored. We were informed that business units monitored systems access, although not consistently. The onus was placed on business units to ensure that access was appropriate. Procedures were in place (linked to the human resource system) to update system access when staff started, moved or left.

While there was reasonable assurance that access was only provided to appropriate staff, we concluded that there was a weakness in the failure to consistently monitor overall system access.

Recommendation 6

We recommend that Treasury reviews monitoring of system access by business units to ensure consistency across all systems.

1.4 Was there a strategic approach to ICT security?

To minimise security risks, ICT management entails:

- having an ICT security plan linked to risk management (Section 1.4.1)
- having appropriate governance — with an information security committee or management group performing that function (Section 1.4.2)
- implementing security in such a way that there was minimal reliance on human actions — e.g. unattended workstations should automatically lock (Section 1.4.3)
- implementing a security incident recording and management system (Section 1.4.4)
- having up-to-date business continuity and disaster recovery plans in the event of a severe or catastrophic ICT security incident. (Section 1.4.5)

1.4.1 Was there an effective ICT security plan and risk management?

The strategic risk review supplied to Audit was completed in 2009 and was under review at the time of the audit.

Treasury had an information security policy but no specific ICT security plan. We noted that a draft information management (including ICT) security plan was being developed.

Recommendation 7

We recommend that Treasury develops a specific ICT security plan and updates its ICT security risk review.

1.4.2 Was there an information security governance and management committee?

The *Tasmanian Government Information Security Manual* specified that entities must have an information security committee composed of senior management or assign the role to an existing senior management committee. Treasury allocated the role to its Executive Management Group and provided us with minutes indicating actions taken on ICT security matters.

We concluded that Treasury had an operational information security management committee function undertaken by its Executive Management Group.

1.4.3 Was effective use made of inbuilt controls?

There should be minimal reliance on staff taking an active role in security. Accordingly, we expected Treasury to have:

- a standard operating environment (SOE)
- automatic timed lockout
- an embargo on unauthorised software
- control over internet access
- control over unauthorised media (all devices containing media, such as external hard drives, cameras, mobile phones, digital audio players and portable media players)
- regularly changing passwords and with enforced standards of strength.

We found that Treasury's SOE prevented installation of unauthorised software. Password strength and complexity was enforced, although audit testing showed some deficiencies in password length and complexity in some applications. Other weaknesses were also identified:

- Automatic timed lockout had been altered to allow users to change the time period from the ten minute default.
- The ICT Security Policy stipulated that only in-house media, USB sticks, portable hard drives, CDs and DVDs were to be used. Despite that requirement, there was no way of enforcing it.

We concluded that Treasury had inbuilt some components of its ICT plan, but there were weaknesses with inconsistent passwords, staff being able to alter the timed lockout and potential use of unauthorised media.

Recommendation 8

We recommend that Treasury makes greater use of inbuilt IT controls such as enforcing password standards and controls over use of unauthorised media.

1.4.4 Was there an incident recording and management system?

Government entities should have a system to record and manage ICT security incidents. Security breaches and near misses should be recorded and analysed in order to facilitate improvements in security.

Treasury had a satisfactory incident recording and management system.

1.4.5 Did business continuity and disaster recovery plans enable maintenance of business functions and security?

An ICT disaster recovery plan and over-arching business continuity plan is needed to enable the department to promptly recover services and continue business in response to a loss of ICT services. Plans should be tested regularly.

We found that Treasury had a disaster recovery policy that set responsibilities for developing and maintaining disaster recovery plans. The disaster recovery plan was presented and maintained on a website.

Treasury's business units developed and maintained their own business continuity plans.

Treasury advised us that ICT equipment was tested when components were changed or replaced with the scale of testing dependent on the magnitude of the update applied.

The policy calls for system disaster recovery testing based on at least annual risk assessments. The last full disaster recovery test weekend occurred in November 2011. We were informed that partial tests have been conducted when there was a change to a component of the ICT system.

Recommendation 9

We recommend that Treasury conducts a full test of its disaster recovery and business continuity plans.

1.5 Conclusion

Treasury had many of the necessary elements of a strategic framework including a high-level governance structure, risk review and policies. However, we did not consider the strategic approach to be fully effective due to the lack of an ICT security plan.

Physical security over ICT did not meet the Australian Government standards that we applied, with weaknesses noted in the areas of policy, construction and CCTV monitoring. Weaknesses were offset to some degree by building security.

With respect to information security, Treasury regularly backed up data and limited access to appropriate staff although some weaknesses were identified. We found cyber security to be deficient because an essential mitigation strategy was missing.

2 Department of Primary Industries, Parks, Water and Environment

2 Department of Primary Industries, Parks, Water and Environment

2.1 Introduction

DPIPWE had an annual budget of over $200m and 1 260 FTEs in 2013–14. The department responsibilities included:

- managing Tasmania's natural resources (i.e. water, air, land, plants, animals and fisheries)
- primary industries and food sectors
- natural and cultural heritage
- land and resource information infrastructure
- access to government services via the Service Tasmania network.

ICT systems played a major role in enabling DPIPWE to carry out its role and we expected:

- physical security over facilities, network infrastructure and servers within DPIPWE buildings (Section 2.2)
- that information kept on ICT systems at DPIPWE was safe and secure (Section 2.3)
- a strategic approach to ICT security. (Section 2.4)

DPIPWE consists of disparate business units. Thus it was a challenge for the department to achieve consistency of ICT policy and practice across many systems and applications.

2.2 *Was there physical security over facilities, network infrastructure and servers, within government buildings?*

In order to assess the effectiveness of physical security to protect server rooms, network infrastructure and other hardware in the department's buildings we examined whether there was:

- effective physical security over server rooms and servers (Section 2.2.1)
- effective physical security over network infrastructure (Section 2.2.2)
- any certification or accreditation regime for ICT physical security. (Section 2.2.3)

Tasmanian Government organisations were to comply with the *Tasmanian Government Identity and Access Management Toolkit* published by DPAC. We also checked compliance with the *Australian Government Physical Security Management Protocol.*

2.2.1 Was there effective physical security over the server room and servers?

We examined whether server rooms and servers had effective alarms, access controls (including control over third parties), intruder detection and hazard protection (fire, flood or power problems) to provide reasonable security over damage to equipment and unauthorised systems access.

DPIPWE's ICT security policy covered physical security, although it was not up-to-date (last revised in 2003).

Examining a number of server rooms, we found satisfactory physical security in all but one server room. However, for that server room we found:

- Access was not controlled swipe-card entry.
- Intruder alarms were not used.
- There was no hazard protection.

We also found one server room was not solidly constructed (i.e. stud walls and suspended ceiling).

Notwithstanding the above observations, access to server rooms required clearing building security or gaining access to the floor with an appropriate swipe-card.

Recommendation 10

We recommend that DPIPWE updates its ICT security policy and upgrades access controls, alarms and hazard protection at specific server rooms where necessary.

2.2.2 Was there effective physical security over network infrastructure?

We expected that there would be control measures to protect network infrastructure such as building cabling, routers and switches. In our view, these items need to be out of sight and secured by basic level locks and keys in order to prevent accidental or malicious damage.

Building cabling observed at DPIPWE sites visited had no specific protection. Some riser shafts inside buildings were locked but in other places, such as basements, cables were exposed and potentially vulnerable. Switches and routers were not subject to any special security measures.

On the basis of our findings, we concluded that improvements could be made to DPIPWE's physical security over network infrastructure.

Recommendation 11

We recommend that DPIPWE provides protective covering for any exposed building cabling and provides basic security of switches and routers.

2.2.3 Were physical facilities certified and accredited?

The *Australian Government Physical Security Management Protocol* calls for a hierarchical security zoning and accreditation for measures taken for each zone.

As noted in Section 1.2.3, there was no process for achieving accreditation at the Tasmanian level and we have recommended in Section 1.2.3 that DPAC implements such a system.

2.3 Was information safe and secure?

Government departments have to protect information. To determine whether that was so, we applied the following criteria to ascertain whether data was:

- backed up effectively (Section 2.3.1)
- safe from cyber-attack (Section 2.3.2)
- accessible only to appropriate staff. (Section 2.3.3)

2.3.1 Was data backed up effectively?

We expected a reliable backup process to:

- be fully documented
- have backup logs
- have safe and appropriate storage with backup tapes kept at a separate location
- test backups regularly.

We found that DPIPWE backed up the 121 servers within its organisation using a priority software program. Backups were logged but we made the following observations:

- Some storage was not off-site although we were informed that the matter was under review.

- Backup tests were performed monthly, quarterly and intermittently for different databases and operating systems.
- We expected a restore testing log to be maintained but this was not so.

Recommendation 12

We recommend that DPIPWE uses off-site storage for all backup tapes. Backup procedures should be recorded and testing logs maintained.

2.3.2 *Was data safe from cyber-attack?*

As mentioned in the Introduction, we tested against ten mitigation strategies from *Strategies to Mitigate Targeted Cyber Intrusions*[12]. Table 5 shows the strategies in number order and our assessments against them. The 'Top 4' are at the head of the Table and are considered by ASD to be essential.

Table 5: Mitigation strategies at DPIPWE

Strategy	Rating
Application whitelisting (listing of trusted programs, not allowing installation of non-trusted software). This is the top strategy because it provides control over malicious programs from any source including emails, USBs and the internet.	✗[1]
Patching applications (monitoring for patches for 'extreme risk' vulnerabilities, timely installation, list software and patches applied)	P[2]
Patching operating system (monitoring for patches for 'extreme risk' vulnerabilities, timely installation, maintain history of patches applied)	P[3]
Minimising users with administrative privileges	✓
Disabling local administrator accounts (involves more than password control)	✗[4]
Application-based workstation firewall	P[5]
Multi-factor authentication (e.g. use of a token and a password)	✓
Network segmentation (partitioning the network) and segregation (rule-based) into security zones to protect	✓

[12] ASD, *Strategies to Mitigate Targeted Cyber Intrusions*., October 2012

Strategy	Rating
sensitive information and critical services	
Host-based intrusion detection/prevention system	✓
Centralised and time-synchronised logging	✓

[1] Not performed, DPIPWE informed us that it had not found software that would allow application whitelisting easily and DPIPWE has multiple business units with various application requirements that would make implementing application whitelisting complex.

[2] Application patching was usually performed monthly, but procedures were not formally documented.

[3] Operating system patching was routinely performed but procedures were not formally documented.

[4] Local administrator accounts, unique to each computer, were not disabled, although password control existed.

[5] Workstation firewalls were only enabled within some areas of the department.

DPIPWE had implemented, or partially implemented, most of the tested mitigation strategies. However, we concluded that data was at medium-high risk at DPIPWE because of the lack of application whitelisting (considered by ASD to be essential) and failure to document patching procedures and to disable local administrator accounts.

Recommendation 13

We recommend that DPIPWE:

- **considers the use of firewalls for workstations throughout the department**
- **disables local administrator accounts.**

We also re-state Recommendation 5 that:

> We recommend that all departments fully implement at least the ‘Top 4’ mitigation strategies from the Australian Signals Directorate publication: *Strategies to Mitigate Targeted Cyber Intrusions.*

2.3.3 Was data access only available to appropriate staff?

We tested for:

- policies and procedures that ensured:
  - staff access to data was limited to a need-to-know basis

  - no superfluous accounts were maintained (in light of staff movements, new starts, transfers and terminations)
- testing, monitoring and logging of access.

We found that DPIPWE did not have an access policy. Staff had access to ICT resources at their manager's approval. All changes to access were instigated from Human Resources (HR), so there was reliance on HR and managers in the organisational units to ensure that access was correct.

We performed sample testing of staff account creation, staff movements and deletions from the ICT system and found no irregularities. However, access controls were not tested or monitored at DPIPWE.

We concluded that access to data was only available to appropriate staff. However, there was a need to develop an access policy and to test and monitor access.

Recommendation 14

We recommend that DPIPWE:

- **develops a policy to ensure that access to confidential information is valid and that no unused accounts exist**
- **implements regular testing and monitoring of user access.**

2.4 Was there a strategic approach to ICT security?

To minimise the security risk, ICT management entails:

- having an ICT security plan linked to risk management (Section 2.4.1)
- having appropriate governance — with an information security committee or management group performing that function (Section 2.4.2)
- implementing security in such a way that there was minimal reliance on human actions — e.g. unattended workstations should automatically lock (Section 2.4.3)
- implementing a security incident recording and management system (Section 2.4.4)
- having up-to-date business continuity and disaster recovery plans in the event of a severe or catastrophic ICT security incident. (Section 2.4.5)

2.4.1 Was there an effective ICT security plan and risk management?

Our expectation was that DPIPWE would have an up-to-date ICT security plan and associated risk management process.

At the time of the audit, the department did not have an ICT security plan. We were advised that, in response to the whole-of-government requirement, the plan was a work in progress. Work to date included a governance model (with delegations and designated information security officers) but there was no risk management plan.

Recommendation 15

We recommend DPIPWE implements an ICT security plan and associated risk management plan.

2.4.2 Did the entity have an information security governance and management committee?

The *Tasmanian Government Information Security Manual* specified that departments must have an information security committee composed of senior management or assign the role to an existing senior management committee.

DPIPWE had an ICT management steering committee with terms of reference that specified that it acts as the department's information security committee. We examined minutes of recent meetings and concluded that the ICT information management steering committee had suitable members and was carrying out the ICT security function.

2.4.3 Was effective use made of inbuilt controls?

There should be minimal reliance on staff taking an active role in security. Accordingly, we expected DPIPWE to have:

- a standard operating environment (SOE)
- automatic timed lockout
- an embargo on unauthorised software
- control over internet access
- control over unauthorised media (all devices containing media, such as external hard drives, cameras, mobile phones, digital audio players and portable media players)
- regularly changing passwords and with enforced standards of strength.

We found that DPIPWE had two main SOEs in place. Computers locked when left unattended and internet access was restricted.

Unauthorised software could not be installed without approval and password strength and complexity was adequate.

The main weakness identified at DPIPWE was that unauthorised media was not controlled.

Recommendation 16

We recommend DPIPWE implements inbuilt control over use of unauthorised media.

2.4.4 Was there an incident recording and management system?

Government agencies should have a system to record and manage ICT security incidents. Security breaches or near misses should be recorded and analysed in order to facilitate improvements in security.

We found that DPIPWE did not have a specific ICT security management system but security incidents were captured by the help desk system. We were informed that there had been no need for a specific incident recording and management system as there had been no security breaches in the last few years.

In any event, such a system was included in the ICT security policy that was being implemented at the time of the audit.

Recommendation 17

We recommend that DPIPWE implements an ICT security incident recording and management system.

2.4.5 Did business continuity and disaster recovery plans enable maintenance of business functions and security?

An ICT disaster recovery plan and over-arching business continuity plan is needed to enable the department to promptly recover services and continue business in response to a loss of ICT services. Plans should be tested regularly.

We found that DPIPWE lacked business continuity or disaster recovery plans. These were described as a work in progress. We were informed that many applications are duplexed and would need little or no intervention if a failure occurred as the duplexed system would take over.

Recommendation 18

We recommend that DPIPWE develops business continuity plans and ICT security disaster recovery plans and tests plans regularly.

2.5 Conclusion

There were significant deficiencies in the department's strategic approach including the lack of:

- an ICT security plan
- a risk management process
- business continuity and disaster recovery plans.

Physical security over ICT did not meet the Australian Government standards that we applied, with weaknesses noted in the areas of policy, access control, alarms and hazard protection. Weaknesses were offset to some degree by building security.

With respect to information security, DPIPWE regularly backed up data and limited access to appropriate staff although some weaknesses were identified.

In the case of cyber security, DPIPWE had implemented or partially implemented most of the tested mitigation strategies. However, we concluded that data at DPIPWE was at medium-high risk because of the lack of application whitelisting (considered by ASD to be essential) and failure to document patching procedures and to disable local administrator accounts.

3 Department of Health and Human Services

3 Department of Health and Human Services

3.1 Introduction

DHHS had an annual budget of $200m in 2013–14 and 2 600 full time equivalent staff (FTEs), not including staff at the state's health organisations[13]. ICT systems play a major role in enabling DHHS to perform its role and we expected:

- effective physical security over facilities, network infrastructure and servers within DHHS buildings (Section 3.2)
- that information kept on ICT systems at DHHS was safe and secure (Section 3.3)
- a strategic approach to ICT security. (Section 3.4)

DHHS was the largest department in the Tasmanian public service and was responsible for over 400 IT systems across its many business units. The department managed a significant amount of confidential data and therefore must be viewed as high risk for ICT security.

3.2 *Was there physical security over facilities, network infrastructure and servers, within government buildings?*

In order to assess the effectiveness of physical security to protect server rooms, network infrastructure and other hardware in DHHS buildings that we examined whether there was:

- effective physical security over server rooms and servers (Section 3.2.1)
- effective physical security over network infrastructure (Section 3.2.2)
- any certification or accreditation regime for ICT physical security. (Section 3.2.3)

Tasmanian Government organisations are required to comply with the *Tasmanian Government Identity and Access. Management Toolkit*. We also checked compliance with the *Australian Government Physical Security Management Protocol.*

[13] The three Tasmanian Health Organisations (THOs) came into existence on 1 July 2012. In regard to ICT assets, the relationship between DHHS and the three THOs is complex. Ownership of the asset is the deciding factor for responsibility.

Although we have excluded THOs from this audit, it does include coverage of common services provided by the department to the THOs.

3.2.1 Was there was effective physical security over the server room and servers?

We examined whether server rooms and servers had effective alarms, access controls (including control over third parties), intruder detection and hazard protection (fire, flood or power problems) to provide reasonable security over damage to equipment and unauthorised systems access.

The DHHS ICT security policy covered physical access, monitoring and incident management.

We found inconsistent levels of physical security with some server rooms no more secure than any other office or storeroom. Specifically, we noted some sites lacked:

- robust construction
- alarm systems
- visitor controls
- CCTV coverage
- hazard protection.

Notwithstanding these observations, access to server rooms required clearing building security or gaining access to the floor with an appropriate swipe-card.

Recommendation 19

We recommend that DHHS upgrades access controls, alarms and hazard protection at specific server rooms where necessary.

3.2.2 Was there was effective physical security over network infrastructure?

We expected that there would be control measures to protect network infrastructure such as building cabling, routers and switches. In our view, these items need to be out of sight and secured by basic level locks and keys in order to prevent accidental or malicious damage.

We found that the sites that we visited had no specific protection for network infrastructure but was secured in part by security features of the buildings in which the items were located.

Recommendation 20

We recommend that DHHS sets standards for physical security and implements specific protections accordingly.

3.2.3 Were physical facilities certified and accredited?

The *Australian Government Physical Security Management Protocol* calls for a hierarchical security zoning and accreditation for measures taken for each zone.

As noted in Section 1.2.3, there was no process for achieving accreditation at the Tasmanian level and we have recommended in Section 1.2.3 that DPAC implements such a system.

3.3 Was information safe and secure?

Government departments have to protect information. To determine whether that was so, we applied the following criteria to ascertain whether data was:

- backed up effectively (Section 3.3.1)
- safe from cyber-attack (Section 3.3.2)
- accessible only to appropriate staff. (Section 3.3.3)

3.3.1 Was data backed up effectively?

We expected an effective backup process to:

- be fully documented
- have backup logs
- have safe and appropriate storage with backup tapes kept at a separate location
- test backups regularly.

We were advised that DHHS used a proprietary software system to administer and manage backups. The system produced backup logs as a report and maintained a full backup history for all servers. Off-site storage was complete for one copy of all backups.

However, we found that DHHS did not systematically test backups. DHHS relied on requests from staff for files to be restored being sufficiently regular to provide assurance that backups were reliable. We considered the lack of systematic testing to be unsatisfactory.

Recommendation 21

We recommend that DHHS tests backups at a frequency commensurate with risk.

3.3.2 Was data safe from cyber-attack?

As mentioned in the Introduction, we tested against ten mitigation strategies from *Strategies to Mitigate Targeted Cyber Intrusions*[14]. Table 6 shows the strategies in number order (the 'Top 4' are at the head of the table) and our assessments against them.

Table 6: Mitigation strategies at DHHS

Strategy	Rating
Application whitelisting (listing of trusted programs, not allowing installation of non-trusted software). This is the top strategy because it provides control over malicious programs from any source including emails, USBs and the internet.	✗[1]
Patching applications (monitoring for patches for 'extreme risk' vulnerabilities, timely installation, list software and patches applied)	P[2]
Patching operating system (monitoring for patches for 'extreme risk' vulnerabilities, timely installation, maintain history of patches applied)	P[3]
Minimising users with administrative privileges	✗[4]
Disabling local administrator accounts (involves more than password control)	✓
Application-based workstation firewall	✗[5]
Multi-factor authentication (e.g. use of a token and a password)	✗[6]
Network segmentation (partitioning the network) and segregation (rule-based) into security zones to protect sensitive information and critical services	P[7]
Host based intrusion detection/prevention system	✓
Centralised and time-synchronised logging	✓

[1] Not performed at DHHS.

[2] Patching varied depending on the application owner.

[3] A consultant engaged by DHHS reported that 73 per cent of servers were automatically updated but there were many outstanding updates on servers requiring manual updates.

[14] ASD, *Strategies to Mitigate Targeted Cyber Intrusions*., October 2012

[4] The consultant's report also found that many old, disabled accounts existed in the system and an audit would be required to identify and remove them.

[5] Not implemented at DHHS.

[6] Not implemented at DHHS although we were advised of plans to implement multi-factor authentication.

[7] The network was protected by external and internal DMZs. The consultant's report cautions that internal DHHS network was poorly segmented.

In our assessment, DHHS data was at high risk from cyber-attack. The department had only fully implemented three of the strategies and none of the essential mitigation strategies had been fully implemented.

Recommendation 22

We recommend that DHHS:

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

We also re-state Recommendation 5 that:

> We recommend that all departments fully implement at least the 'Top 4' mitigation strategies from the Australian Signals Directorate publication: *Strategies to Mitigate Targeted Cyber Intrusions.*

3.3.3 Was data access only available to appropriate staff?

We tested for:

- policies and procedures that ensured:
  - staff access to data was limited to a need-to-know basis
  - no superfluous accounts were maintained (in light of staff movements, new starts, transfers and terminations)
- testing, monitoring and logging of access.

We found that DHHS used a software product to facilitate user and manager control of access to applications. Despite this, testing performed as a component of financial audit (by the

Tasmanian Audit Office) found that a large number of users — over 2000 — existed in the system that had not logged in at all in 2014[15]. Moreover, there were instances of users that had not logged in from as far back as 2008–2011. It seemed very likely that these users were no longer part of the department.

DHHS indicated that there was no access testing or monitoring.

Recommendation 23

We recommend that DHHS:

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

3.4 Was there a strategic approach to ICT security?

To minimise the security risk, ICT management entails:

- having an ICT security plan linked to a risk management process (Section 3.4.1)
- having appropriate governance — with an information security committee or management group performing that function (Section 3.4.2)
- implementing security in such a way that there was minimal reliance on human actions — e.g. unattended workstations should automatically lock (Section 3.4.3)
- implementing a security incident management and recording system (Section 3.4.4)
- having up-to-date business continuity and disaster recovery plans in the event of a severe or catastrophic ICT security incident. (Section 3.4.5)

3.4.1 Was there an effective ICT security plan and risk management?

We expected that DHHS would have had an up-to-date ICT security plan and associated risk management process.

However, we found neither. A consultant's report (see Section 3.3.2) had made a number of recommendations to improve ICT security and we were informed that the

[15] This figure included the THOs.

department intended to implement those recommendations. There was a list of risks that the senior management group considered at each meeting, but no formal risk register or mitigation planning.

The IT security policy covered off some areas but did not specify an IT security committee, links to any risk assessment, include any resource management or connection to any business continuity planning.

The policy documents were two years old at the time of audit.

Recommendation 24

We recommend that DHHS implements an ICT security plan and associated risk management plan.

3.4.2 Did the entity have an information security governance and management committee?

The *Tasmanian Government Information Security Manual* specified that entities must have an information security committee composed of senior management or assign the role to an existing senior management committee.

While DHHS did not have a dedicated information security committee, governance of ICT security was covered by the Executive Management Group.

3.4.3 Was effective use made of inbuilt controls?

There should be minimal reliance on staff taking an active role in security. Accordingly, we expected DHHS to have:

- a standard operating environment (SOE)
- automatic timed lockout
- an embargo on unauthorised software
- control over internet access
- control over unauthorised media (all devices containing media, such as external hard drives, cameras, mobile phones, digital audio players and portable media players)
- regularly changing passwords and with enforced standards of strength.

We found that DHHS had SOEs and unauthorised software could only be installed with approval of the local administrator. Password strength, and frequency of requirement for users to change their passwords, was adequate but we noted that password complexity rules were not enforced. Another weakness that we identified at DHHS was that unauthorised media was not controlled.

We concluded that some security components were inbuilt at DHHS but there was room for improvement.

Recommendation 25

We recommend that DHHS makes greater use of inbuilt IT controls such as enforcing password standards and controls over use of unauthorised media.

3.4.4 *Was there an incident recording and management system?*

DHHS should have a system to record and manage ICT security incidents. Security breaches and near misses should have been recorded and analysed in order to facilitate improvements in security.

We found that DHHS had an incident management system designed to work for all incidents, not just ICT security. However, the system was:

- overly complicated and poorly documented
- in draft form only and there was no evidence that any recording and analysis was taking place
- without facility to record near misses.

Accordingly, we concluded that the incident recording and management system was unsatisfactory in its current form.

Recommendation 26

We recommend that DHHS rationalises its incident management system and develops a means of specifically recording and analysing ICT security incidents and near misses.

3.4.5 *Did business continuity and disaster recovery plans enable maintenance of business functions and security?*

An ICT disaster recovery plan and over-arching business continuity plan is needed to enable the department to promptly recover services and continue business in response to a loss of ICT services. Plans should be tested regularly.

We found that DHHS did not have over-arching business continuity and disaster recovery plans at the time of the audit, although work was being done in that area. The department was moving towards operating dual data centres, providing redundancy and therefore recovery in the event of ICT failure.

Recommendation 27

We recommend that while DHHS implements its dual data centre approach, the department should produce business continuity and disaster recovery plans and test them regularly.

3.5 Conclusion

There were significant deficiencies in the department's strategic approach including the lack of:

- an ICT security plan
- a risk management process
- business continuity and disaster recovery plans.

Physical security over ICT did not meet the Australian Government standards that we applied, with weaknesses noted in the areas of construction, alarms, visitor controls, CCTV monitoring and hazard protection. Weaknesses were offset to some degree by building security.

With respect to information security, DHHS regularly backed up data although the department did not systematically test backups. While access to data was restricted to appropriate staff, lack of monitoring and testing detracted from assurance that the controls were effective.

In our assessment, DHHS data was at high risk from cyber-attack. The department had only fully implemented three of the strategies and none of the essential mitigation strategies had been fully implemented.

4 Department of Premier and Cabinet

4 Department of Premier and Cabinet

4.1 Introduction

The Department of Premier and Cabinet has around 300 FTEs and an annual budget of approximately $110m in 2013–14. DPAC is responsible for:

- providing support for executive decision making
- e-services for Government agencies and the community
- state service management
- community and local government development.

Within DPAC, TMD and the Office of eGovernment have responsibility for whole-of-government ICT service provision and policy development.

ICT systems play a major role in enabling DPAC to perform its role and we expected:

- effective physical security over facilities, network infrastructure and servers within DPAC buildings (Section 4.2)
- that information kept on ICT systems at DPAC was safe and secure. (Section 4.3)
- a strategic approach to ICT security. (Section 4.4)

Since DPAC included TMD and the Office of eGovernment, we expected that it would be the flagship for ICT security management.

4.2 Was there physical security over facilities, network infrastructure and servers, within government buildings?

In order to assess the effectiveness of physical security to protect server rooms, network infrastructure and other hardware in government buildings we examined whether there was:

- effective physical security over server rooms and servers (Section 4.2.1)
- effective physical security over network infrastructure (Section 4.2.2)
- any certification or accreditation for ICT physical security. (Section 4.2.3)

Tasmanian Government entities are to comply with the *Tasmanian Government Identity and Access Management Toolkit*.

We also checked compliance with the *Australian Government Physical Security Management Protocol.*

4.2.1 Was there was effective physical security over the server room and servers?

We examined whether server rooms and servers had effective alarms, access controls (including control over third parties), intruder detection and hazard protection (fire, flood or power problems) to provide reasonable security over damage to equipment and unauthorised systems access.

DPAC's ICT security policy included minimal coverage of physical security. Nonetheless, we found that reasonable controls existed over server rooms and servers. Greater security could be achieved by:

- more robust construction of server rooms
- expanded use of CCTV coverage
- hazard protection.

Recommendation 28

We recommend that DPAC upgrades its coverage of physical security in its ICT security policy. We also recommend that DPAC reviews construction of server rooms, expanded use of CCTV and greater hazard protection.

4.2.2 Was there effective physical security over network infrastructure?

We expected that there would be control measures to protect network infrastructure such as building cabling, routers and switches. In our view, these items need to be out of sight and secured by basic level locks and keys in order to prevent accidental or malicious damage.

We found that building cabling and network infrastructure at sites visited had no specific in-building protection but was secured in part by security features of the buildings in which the items were located.

Recommendation 29

We recommend that DPAC sets standards for physical security and implements specific protections accordingly.

4.2.3 Were physical facilities certified and accredited?

The *Australian Government Physical Security Management Protocol* calls for a hierarchical security zoning and accreditation for measures taken for each zone.

As noted in Section 1.2.3, there was no process for achieving accreditation at the Tasmanian level and we have recommended in Section 1.2.3 that DPAC implements such a system.

4.3 Was information safe and secure?

Government departments have to protect information. To determine whether that was so, we applied the following criteria to ascertain whether data was:

- backed up effectively (Section 4.3.1)
- safe from cyber-attack (Section 4.3.2)
- accessible only to appropriate staff. (Section 4.3.3)

4.3.1 Was data backed up effectively?

We expected a reliable backup process to:

- be fully documented
- have backup logs
- have safe and appropriate storage with backup tapes kept at a separate physical location
- test backups regularly.

DPAC's backup regime proved to be satisfactory although we noted some weaknesses:

- Backup tape procedure appeared to have been written specifically for our audit.
- Staff provided examples of help desk jobs indicating that restores of data had worked. Although staff claimed to test backups bi-monthly, no documentation was provided to support that assertion.

Recommendation 30

We recommend that DPAC tests backups and retains test documentation to provide assurance that restores will function correctly.

4.3.2 Was data safe from cyber-attack?

As mentioned in the Introduction, we tested against ten mitigation strategies from *Strategies to Mitigate Targeted Cyber Intrusions*[16]. Table 7 shows the strategies in number order (the 'Top 4' are at the head of the table) and our assessments against them.

Table 7: Mitigation strategies at DPAC

Strategy	Rating
Application whitelisting (listing of trusted programs, not allowing installation of non-trusted software). This is the top strategy because it provides control over malicious programs from any source including emails, USBs and the internet.	✗[1]
Patching applications (monitoring for patches for 'extreme risk' vulnerabilities, timely installation, list software and patches applied)	✗[2]
Patching operating system (monitoring for patches for 'extreme risk' vulnerabilities, timely installation, maintain history of patches applied)	✗[3]
Minimising users with administrative privileges	✓
Disabling local administrator accounts (involves more than password control)	✗[4]
Application-based workstation firewall	✓
Multi-factor authentication (e.g. use of a token and a password)	✓
Network segmentation (partitioning the network) and segregation (rule-based) into security zones to protect sensitive information and critical services	✓
Host based intrusion detection/prevention system	✓
Centralised and time-synchronised logging	✓

[1] DPAC does not use application whitelisting but does use an SOE to provide limitations on software in use.

[2], [3] Regular patching of workstations was performed but was 'ad-hoc' for server-based applications and operating systems. DPAC advised that it was moving to a proprietary patching regime.

[16] ASD, *Strategies to Mitigate Targeted Cyber Intrusions*., October 2012

[4] Local administrator accounts, unique to each computer, were not disabled, although password control existed.

In our assessment, DPAC data was at medium-high risk from cyber-attack. The department had not fully implemented three of the essential strategies although most of the other mitigation strategies were being used.

Recommendation 31

We recommend that DPAC disables local administrator accounts.

We re-state Recommendation 5 that:

> We recommend that all departments fully implement at least the 'Top 4' mitigation strategies from the Australian Signals Directorate publication: *Strategies to Mitigate Targeted Cyber Intrusions*.

4.3.3 Was data access only available to appropriate staff?

We tested for:

- policies and procedures that ensured:
  - staff access to data was limited to a need-to-know basis
  - no superfluous accounts were maintained (in light of staff movements, new starts, transfers and terminations)
- testing, monitoring and logging of access.

We found that DPAC's ICT security policy specified that access to systems and applications should be based on business needs and had to be authorised by a senior manager.

We reviewed departmental testing of access to data and were satisfied that data access was only available to appropriate staff. We also found that permissions were current, although we noted some departures from policy with respect to password strength and history.

Recommendation 32

We recommend that DPAC enforces its password parameters in line with departmental policy.

4.4 Was there a strategic approach to ICT security?

ICT management to minimise security risk entails:

- having an ICT security plan linked to a risk management process (Section 4.4.1)

- having appropriate governance — with an information security committee or management group performing that function (Section 4.4.2)
- implementing security in such a way that there was minimal reliance on human actions — e.g. unattended workstations should automatically lock (Section 4.4.3)
- implementing a security incident management and recording system (Section 4.4.4)
- having up-to-date business continuity and disaster recovery plans in the event of a severe or catastrophic ICT security incident. (Section 4.4.5)

4.4.1 *Was there an effective ICT security plan and risk management?*

We expected DPAC to have an up-to-date ICT security plan with an associated risk management process.

DPAC had an ICT security policy but no specific ICT security plan. We noted that risk management documentation was satisfactory.

Recommendation 33

We recommend DPAC develops a specific ICT security plan.

4.4.2 *Was there an information security governance and management committee?*

The *Tasmanian Government Information Security Manual* specified that agencies must have an information security committee composed of senior management or assign the role to an existing senior management committee.

After examining the role of DPAC's Information Security Advisory Group, we concluded that it fulfilled the above-mentioned requirement.

4.4.3 *Was effective use made of inbuilt controls?*

There should be minimal reliance on staff taking an active role in security. Accordingly, we expected DPAC to have:

- a standard operating environment (SOE)
- automatic timed lockout
- an embargo on unauthorised software
- control over internet access
- control over unauthorised media (all devices containing media, such as external hard drives, cameras, mobile phones, digital audio players and portable media players)

- regularly changing passwords and with enforced standards of strength.

The department had an SOE. ICT staff managed computers using a software system that provided remote control, patch management, software distribution, operating system deployment, network access protection and an inventory for hardware and software. In addition, we found DPAC monitored internet access.

According to DPAC's workstation and portable devices security policy, users were required to lock their computers themselves when devices were to be left unattended.

Unauthorised software was not controlled, although software could not be installed without administrator access. Unauthorised media was not controlled.

There was a discrepancy between the password strength in the ICT security policy and the submitted password standards in use as discussed in Section 4.3.3. We concluded that more could be done to make requirements of the plan inbuilt at DPAC.

Recommendation 34

We recommend that DPAC makes greater use of inbuilt IT features such as time-outs on personal computers, enforcing password standards, controls over unauthorised media and software.

4.4.4 Was there an incident recording and management system?

Government entities should have systems to record and manage ICT security incidents. Security breaches and near misses should be recorded and analysed in order to facilitate improvements in security.

We found that DPAC used its help desk system to record and monitor security incidents. That system provided a procedure to log security incidents and to monitor and report them. However, the system did not allow for recording near misses.

Recommendation 35

We recommend that DPAC modifies its help desk system to enable it to record security near misses.

4.4.5 Did business and disaster continuity plans enable maintenance of business functions and security?

An ICT disaster recovery plan and over-arching business continuity plan is needed to enable the department to promptly recover services and continue business in response to a loss of ICT services. Plans should be tested regularly.

We reviewed the DPAC business continuity plan and server disaster recovery plan.

The server disaster continuity plan had areas that could be improved in that it did not specifically identify responsible officers, was not linked to risk management documentation, did not cover security breaches or cyber-attack and had no recovery time objectives.

DPAC had no documentation to support testing of the plans. We were advised that there was a planned test before December 2014.

Recommendation 36

We recommend that DPAC improves its disaster recovery plan by identifying responsible officers, linking to risk management documentation, covering security breaches and cyber-attacks as well as setting recovery time objectives.

We further recommend that the department documents tests of its disaster recovery plan.

4.5 Conclusion

There were significant deficiencies in the department's strategic approach including:

- lack of an ICT security plan
- lack of automatic locking on workstations and portable devices
- lack of controls over unauthorised software and media
- gaps in its disaster recovery plans.

Physical security over ICT did not meet the Australian Government standards that we applied, with weaknesses noted in the areas of policy, construction, CCTV monitoring and hazard protection. Weaknesses were offset to some degree by building security.

With respect to information security, DPAC regularly backed up data although the department did not systematically test backups nor retain test documentation. While access to data was restricted to appropriate staff, the department had not enforced its password parameters. Also the security policy should require testing and monitoring of access controls.

In our assessment, DPAC data was at medium-high risk from cyber-attack. The department had not fully implemented three of the essential strategies although most of the other mitigation strategies were being used.

5 Department of Police and Emergency Management

5 Department of Police and Emergency Management

5.1 Introduction

The Department of Police and Emergency Management had a budget of over $200m in 2013–14 and over 1 500 full-time equivalent staff (FTEs). The department also used the services of some 500 emergency service volunteers.

DPEM has public safety, fighting crime, policing traffic and emergency management as its major responsibilities.

ICT systems play a crucial role in enabling DPEM to perform its role and we expected that there would be:

- physical security over facilities, network infrastructure and servers within DPEM buildings (Section 5.2)
- that information kept on ICT systems at DPEM was safe and secure (Section 5.3)
- a strategic approach to ICT security. (Section 5.4)

Due to the nature of its policing and emergency service responsibilities, DPEM had a high exposure to failure of ICT systems and communications as well as susceptibility to malicious attack. We expected that DPEM would have high standards of ICT security.

5.2 Was there physical security over facilities, network infrastructure and servers, within government buildings?

In order to assess the effectiveness of physical security to protect server rooms, network infrastructure and other hardware in DPEM buildings we examined whether there was:

- effective physical security over server rooms and servers (Section 5.2.1)
- effective physical security over network infrastructure (Section 5.2.2)
- any certification or accreditation for ICT physical security. (Section 5.2.3)

Tasmanian government entities are to comply with the *Tasmanian Government Identity and Access Management Toolkit*. We also checked compliance with the *Australian Government Physical Security Management Protocol.*

5.2.1 Was there effective physical security over the server room and servers?

We examined whether server rooms and servers had effective alarms, access controls (including control over third parties), intruder detection and hazard protection (fire, flood or power problems) to provide reasonable security over damage to equipment and unauthorised systems access.

We found that DPEM had a policy that contained clear objectives and standards as well as covering various aspects of physical security.

We inspected a number of DPEM ICT sites that ranged from large data centres to office server rooms. Security was generally strong with sectionalised access that worked particularly well.

5.2.2 *Was there effective physical security over network infrastructure?*

We expected that there would be control measures to protect network infrastructure such as building cabling and routers. In our view, these items need to be out of sight and secured by basic level locks and keys in order to prevent accidental or malicious damage.

Two of the facilities visited were data centres where we noted protection for building cabling. Other sites — one at a police station and the other at an office — were similar to those visited in other entities in that there was no special protection for network cabling, routers and switches, other than the security the building offered.

Recommendation 37

We recommend that DPEM sets standards for physical security and implements specific protections accordingly.

5.2.3 *Were physical facilities certified and accredited?*

The *Australian Government Physical Security Management Protocol* calls for a hierarchical security zoning and accreditation for measures taken for each zone.

As noted in Section 1.2.3, there was no process for achieving accreditation at the Tasmanian level and we have recommended in Section 1.2.3 that DPAC implements such a system.

5.3 *Was information safe and secure?*

Government departments have to protect information. To determine whether that was so, we applied the following criteria to ascertain whether data was:

- backed up effectively (Section 5.3.1)

- safe from cyber-attack (Section 5.3.2)
- accessible only to appropriate staff. (Section 5.3.3)

5.3.1 Was data backed up effectively?

We expected an effective backup process to:

- be fully documented
- have backup logs
- have safe and appropriate storage with backup tapes stored at a separate location
- test backups regularly.

We found that the DPEM ICT security plan had a chapter on operations management that incorporated data and system backup. The plan stipulated that backup and complementary restore procedures were based on a risk assessment for each system and were regularly proven to meet business and legal requirements.

We examined backup and restore logs together with tape storage. We verified that backups and restores were implemented. One weakness we identified was that procedures were not documented as required by the plan.

Recommendation 38

We recommend that DPEM documents its backup and restore procedures.

5.3.2 Was the data safe from cyber-attack?

As mentioned in the Introduction, we tested against ten mitigation strategies from *Strategies to Mitigate Targeted Cyber Intrusions*[17]. Table 8 shows the strategies in number order (the 'Top 4' are at the head of the Table) and our assessments against them.

[17] ASD, *Strategies to Mitigate Targeted Cyber Intrusions*., October 2012

Table 8: Mitigation strategies at DPEM

Strategy	Rating
Application whitelisting (listing of trusted programs, not allowing installation of non-trusted software). This is the top strategy because it provides control over malicious programs from any source including emails, USBs and the internet.	✗[1]
Patching applications (monitoring for patches for 'extreme risk' vulnerabilities, timely installation, list software and patches applied)	✗[2]
Patching operating system (monitoring for patches for 'extreme risk' vulnerabilities, timely installation, maintain history of patches applied)	✗[3]
Minimising users with administrative privileges	✓
Disabling local administrator accounts (involves more than password control)	✗[4]
Application-based workstation firewall	✗[5]
Multi-factor authentication (e.g. use of a token and a password)	✓
Network segmentation (partitioning the network) and segregation (rule-based) into security zones to protect sensitive information and critical services	✓
Host based intrusion detection/prevention system	✓
Centralised and time-synchronised logging	✓

[1] We were advised that application whitelisting was being investigated.

[2] Patching of application software was required by the ICT Security Plan but no written procedures or documentary evidence was supplied.

[3] Patching of operating systems was performed monthly rather than in response to patches being made available.

[4] Local administrator accounts, unique to each computer, were not disabled, although password control existed.

[5] No application-based firewalls were used.

In our assessment, DPEM data was at high risk from cyber-attack. The department had not fully implemented three of the essential strategies although most of the other mitigation strategies were being used.

Recommendation 39

We recommend that DPEM:

- **disables local administrator accounts**
- **implements application-based firewalls.**

We also re-state Recommendation 5 that:

> We recommend that all departments fully implement at least the 'Top 4' mitigation strategies from the Australian Signals Directorate publication: *Strategies to Mitigate Targeted Cyber Intrusions.*

5.3.3 Was data access only available to appropriate staff?

We tested for:

- policies and procedures that ensured:
  - staff access to data was limited to a need-to-know basis
  - no superfluous accounts were maintained (in light of staff movements, new starts, transfers and terminations)
- testing, monitoring and logging of access.

We found that DPEM's ICT security plan specified role-based access control but there was no:

- procedure for staff new starts, movements, terminations or access for contractors
- formal testing other than for highly sensitive systems or upon request.

We performed testing on a sample of staff starts, movements and terminations and found no irregularities with access management.

In summary, we have reasonable confidence from testing that access was appropriately controlled but had concerns about documentation, monitoring and testing.

Recommendation 40

We recommend that DPEM fully documents its access procedures and implements a regular program of access testing.

5.4 Was there a strategic approach to ICT security?

To minimise security risks, ICT management entails:

- having an ICT security plan linked to risk management (Section 5.4.1)

- having appropriate governance — with an information security committee or management group performing that function (Section 5.4.2)
- implementing security in such a way that there was minimal reliance on human actions e.g. unattended workstations should automatically lock (Section 5.4.3)
- implementing a security incident management and recording system (Section 5.4.4)
- having up-to-date business continuity and disaster recovery plans in the event of a severe or catastrophic ICT security incident. (Section 5.4.5)

5.4.1 *Was there an effective ICT security plan and risk management?*

We tested to confirm whether DPEM had an up-to-date ICT security plan and associated risk management process. The DPEM ICT security plan supplied was comprehensive, covering 21 areas including, for example:

- information security classification system
- physical security
- network and communications management
- acquisition, development and maintenance of systems
- use of cryptography to protect sensitive data.

We noted one weakness, though, in that the plan did not stipulate regular review of risks.

Recommendation 41

We recommend that DPEM specifies in its ICT security plan that risk reviews should take place regularly.

5.4.2 *Was there an information security governance and management committee?*

The *Tasmanian Government Information Security Manual* specified that agencies must have an information security committee composed of senior management or assign the role to an existing senior management committee.

At DPEM there was a suitably staffed information security committee and we sighted its terms of reference and minutes of various meetings.

5.4.3 *Was effective use made of inbuilt controls?*

There should be minimal reliance on staff taking an active role in security. Accordingly, we expected DPEM to have:

- a standard operating environment (SOE)
- automatic timed lockout
- an embargo on unauthorised software
- control over internet access
- control over unauthorised media (all devices containing media, such as external hard drives, cameras, mobile phones, digital audio players and portable media players)
- regularly changing passwords and with enforced standards of strength.

We found that the department had an SOE and automatic timed lockout although we noted that the time interval was set at one hour which we considered to be excessive.

However, the department did not use inbuilt controls over unauthorised software, internet access and unauthorised media.

We concluded that DPEM had not optimised the use of inbuilt IT controls.

Recommendation 42

We recommend that DPEM makes greater use of inbuilt IT controls such as controls over unauthorised software, media and internet access.

5.4.4 Were there an incident recording and management system?

Government agencies should have a system to record and manage ICT security incidents. Security breaches and near misses should be recorded and analysed in order to facilitate improvements in security.

At DPEM, the ICT security plan required effective processes for detecting, reporting, recording and resolving ICT security incidents. However, DPEM were unable to supply evidence of a recording system or that incidents had been recorded.

Recommendation 43

We recommend that DPEM implements an IT security incident management and recording system.

5.4.5 Did business continuity and disaster recovery plans enable maintenance of business functions and security?

An ICT disaster recovery plan and over-arching business continuity plan is needed to enable the department to promptly recover services and continue business in response to a loss of ICT services. Plans should be tested regularly.

Despite a requirement of the 2008 ICT Security Plan to:

> have an approved, implemented, published Business Continuity Plan supported by relevant procedures that are regularly reviewed …

no such plan existed. The department was also unable to provide a disaster recovery plan, although we were advised that plans were being developed.

Recommendation 44

We recommend that DPEM formalises, implements and tests business continuity and disaster recovery plans.

5.5 Conclusion

DPEM had a comprehensive ICT security plan and governance structure. However, there were deficiencies in the department's strategic approach including the lack of:

- an incident recording and management system
- business continuity and disaster recovery plans.

Physical security was found to be satisfactory in all respects.

In our assessment, DPEM data was at high risk from cyber-attack. The department had not fully implemented three of the essential strategies although most of the other mitigation strategies were being used.

With respect to information security, DPEM regularly backed up data. In addition, access to data appeared to be appropriately restricted although there was a lack of documentation of testing access control.

This page left blank intentionally

Independent auditor's conclusion

Independent auditor's conclusion

This independent conclusion is addressed to the President of the Legislative Council and to the Speaker of the House of Assembly.

It relates to my performance audit assessing how well selected government departments managed their ICT infrastructure.

Audit objective

The objective of the audit was to assess the effectiveness of security measures for ICT infrastructure in government departments.

Audit scope

The audit included ICT physical infrastructure, applications and information. Departments subject to audit were:

- Treasury and Finance (Treasury)
- Primary Industries, Parks, Water and Environment (DPIPWE)
- Health and Human Services (DHHS)
- Premier and Cabinet (DPAC)
- Police and Emergency Management (DPEM).

Responsibility of the five Secretaries

The Secretaries of the five departments selected for audit are responsible for implementing processes to ensure effective security measures exist and are implemented regarding their ICT infrastructure.

Auditor-General's responsibility

In the context of this performance audit, my responsibility was to express a conclusion on the effectiveness of the ICT infrastructure security measures implemented by the five departments selected for audit.

I conducted my audit in accordance with Australian Auditing Standard ASAE 3500 *Performance engagements*, which required me to comply with relevant ethical requirements relating to audit engagements. I planned and performed the audit to obtain reasonable assurance that the Secretaries had implemented effective security measures for their ICT infrastructure.

My work involved, in line with the audit criteria documented on Page 25, the audit involved:

- questionnaires completed by audit clients

- review of policies and other documentation
- site visits
- testing
- interviews.

The audit also used benchmarks from the:

- Australian Information Commission
- Australian Government Information Security Manual[18]
- *Tasmanian Government Identity and Access Management Toolkit*[19]
- *Australian Government Physical Security Management Protocol.*

I believe that the evidence I obtained was sufficient and appropriate to provide a basis for my conclusion.

Auditor-General's conclusion

Based on the audit objective and scope and for reasons outlined in this Report, it is my conclusion that, in all material respects, departments had reasonable security over most of their facilities, infrastructure and servers and information was generally safe and secure with reasonable back-up and access restrictions.

However, there:

- were areas of inadequate security at most departments
- was excessive risk from cyber-attacks
- was wide-spread failure to take a strategic approach.

To improve security I made 44 recommendations most of which are aimed at specific departments and others at all departments.

H M Blake

Auditor-General

26 March 2015

[18] The Guide contains a section on ICT Security measures. The ASD produces the *Information Security Manual* that contains controls for ICT security.

[19] Published by the Office of eGovernment in the Department of Premier and Cabinet.

This page left blank intentionally

Recent reports

Recent reports

Tabled	No.	Title
Dec	No.4 of 2013–14	Financial Statements of State entities, Volume 3 — Local Government Authorities
Dec	No.5 of 2013–14	Infrastructure Financial Accounting in Local Government
Jan	No. 6 of 2013–14	Redevelopment of the Royal Hobart Hospital: governance and project management
Feb	No. 7 of 2013–14	Police responses to serious crime
Feb	No. 8 of 2013–14	Financial Statements of State entities, Volume 4 Analysis of the Treasurer's Annual Financial Report 2012–13
May	No.9 of 2013–14	Financial Statements of State entities, Volume 5 — State entities 30 June and 31 December 2013, matters relating to 2012–13 audits and key performance indicators
May	No.10 of 2013–14	Government radio communications
May	No.11 of 2013–14	Compliance with the Alcohol, Tobacco and Other Drugs Plan 2008–13
June	No.12 of 2013–14	Quality of Metro services
June	No. 13 of 2013–14	Teaching quality in public high schools
Aug	No. 1 of 2014–15	Recruitment practices in the Tasmanian State Service
Sep	No. 2 of 2014–15	Follow up of selected Auditor-General reports: October 2009 to September 2011
Sep	No 3 of 2014–15	Motor vehicle fleet management in government departments
Nov	No. 4 of 2014–15	Financial Statements of State entities, Volume 3: Government Businesses 2013–14
Nov	No. 5 of 2014–15	Financial Statements of State entities, Volume 2 — General Government and Other State entities 2013–14
Dec	No. 6 of 2014–15	Financial Statements of State entities, Volume 1 — Analysis of the Treasurer’s Annual Financial Report 2013–14
Feb	No.7 of 2014–15	Report No. 7 Financial Statements of State entities, Volume 4 — Local Government Authorities, Joint Authorities and Tasmanian Water and Sewerage Corporation Pty Ltd 2013-14

Current projects

Current projects

The table below contains details performance and compliance audits that the Auditor-General is currently conducting and relates them to the *Annual Plan of Work 2014–15* that is available on our website. Items marked with an asterisk (*) were underway as at 27 June 2014.

Title	Audit objective is to …	*Annual Plan of Work 2014–15* reference
Vehicle fleet usage and management in government businesses	… review the efficiency and effectiveness of the use of motor vehicles, and testing compliance with applicable guidelines by: government businesses, University of Tasmania and the Retirement Benefits Fund. In addition, it will include the management of vehicle workshops.	Page 20 Topic No. 5
Capital works programming and management	… assess the effectiveness of the state's capital works and ICT budgeting program and departmental asset, including ICT assets, management processes.	Page 18 Topic No. 6*
Management of local government roads	… assess local governments' management of roads with emphasis on maintenance, decision-making on new roads and the level of administration costs that underpin road construction.	Page 20 Topic No. 6
Number of government primary schools	… analyse the efficiency and effectiveness of the current number and location of government primary schools in Tasmania.	Page 19 Topic No. 2
Provision of social housing	… form conclusions as to the effectiveness, efficiency and economy of the provision of social housing and other government assistance provided by Housing Tasmania and non-government organisations to Tasmanians in housing stress	Page 21 Topic No. 7

Title	Audit objective is to …	*Annual Plan of Work 2014–15* reference
Follow-up audit	… ascertain the extent to which recommendations contained in the *2013 Tasmanian Bushfires Inquiry* have been implemented. In addition, follow up the implementation of recommendations contained in *Special Report 99 Bushfire management* and those recommendations contained in *Financial Audit Services Report No. 11 of 2012–13* that relate to the Department of Health and Human Services and the three Tasmanian Health Organisations.	Page 22 Topic No. 9

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) 6226 0100	**Address**	Level 4, Executive Building
Fax	(03) 6226 0199		15 Murray Street, Hobart
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) 6336 2503	**Address**	2nd Floor, Henty House
Fax	(03) 6336 2908		1 Civic Square, Launceston