

# ***Financial Systems Controls Report: Information Technology 2014–15***

Tabled 7 October 2015

The Auditor-General provides assurance to Parliament on the accountability and performance of the Victorian Public Sector. The Auditor-General conducts financial audits and performance audits, and reports on the results of these audits to Parliament.

On 7 October 2015, the Acting Auditor-General tabled his financial audit report, *Financial Systems Controls Report: Information Technology 2014–15*.

## Overview

2

This report summarises the results of our audits of public sector entities' information technology (IT) general controls performed in support of VAGO's 2014–15 financial audits.

We found:

- our financial audits continue to identify a large number of IT control deficiencies
- most of the IT audit findings identified were rated medium and high risk, with one rated as an extreme risk
- there are three clear emerging themes.

This report summarises the results of our audits of public sector entities' information technology (IT) general controls performed in support of VAGO's 2014–15 financial audits.

We found that:

- our financial audits continue to identify a large number of IT control deficiencies, which have the potential to impact the confidentiality, integrity and availability of public sector financial data and IT systems
- most of the 462 IT audit findings identified were rated medium and high risk, with one rated as an extreme risk
- there are three clear emerging themes or trends.

## Background

3

- Financial audits provide independent assurance to Parliament and the community that the information contained in an agency's financial statements is fairly presented in accordance with Australian accounting standards and applicable legislation.
- When planning a financial audit, VAGO seeks to evaluate an entity's IT environment and any related risks to the reliability of financial reporting.

Financial audits provide independent assurance to Parliament and the community that the information contained in an agency's financial statements is fairly presented in accordance with Australian accounting standards and applicable legislation.

When planning a financial audit, VAGO seeks to evaluate an entity's IT environment and related risks to the reliability of financial data and reporting.

## Focus of this report

This audit summarises:

- the results of our audits of public sector entities' IT general controls performed in support of VAGO's 2014–15 financial audits
- reviews performed over focus areas of identity and access management, and software licensing.

The objective of this audit was to:

- provide additional insight into and more visibility of our IT audit findings
- provide decision-makers with relevant information to assist them to address audit findings and improve processes.

The objectives of the Financial Systems Controls Report are to:

- summarise the results of our audits of public sector entities' IT general controls as part of the 2014–15 financial audits and the reviews performed over focus areas of identity and access management, and software licensing
- provide additional insight into and more visibility of our IT audit findings
- provide decision makers with relevant information to assist them to address audit findings and improve processes.

All findings used for this report have been previously communicated to governance bodies and accountable officers via audit 'management letters'.

## Scope and coverage

- 45 selected entities across government.
- 65 key financial applications were audited.



For this audit, 45 entities across government with a financial year end-date of either 31 December 2014 or 30 June 2015 were selected for analysis.

Further insights are provided for our findings at entities within the top four sectors.

Collectively, 65 key financial IT applications and their associated infrastructure were audited.

## Themes from IT audits

Themes were identified through our 2014–15 financial year IT audits

1. The management of controls at outsourced IT environments requires attention.

2. The use of IT systems that are at their end-of-life needs to be addressed.

3. IT security controls need improvement.

**For the 2014–15 financial year, there are three clear emerging themes.**

For the 2014–15 financial year, we identified three clear emerging themes from IT audits.

These are:

- the management of controls at outsourced IT environments requires attention
- the use of IT systems that are at their end-of-life needs to be addressed
- IT security controls need improvement.



## Results of IT audits

- 462 IT audit findings—both new and open from the prior year.
- Most of the IT audit findings identified were rated medium and high risk, with one ranked as an extreme risk.
- 41% of prior-period IT audit findings have not been remediated, many of which were rated high-risk.

**More focused attention and oversight by accountable officers and governance bodies is required to address our IT audit findings.**

Our financial audits continue to identify a large number of IT control deficiencies. 462 IT audit findings were identified in the 2014–15 financial year. This is an increase of 27 percent from the prior year.

Consistent with prior years, most audit findings were rated as medium risk and high risk.

One extreme-risk rated finding was identified during the 2014–15 period. This is in contrast to the previous year's report where no extreme-rated findings were raised.

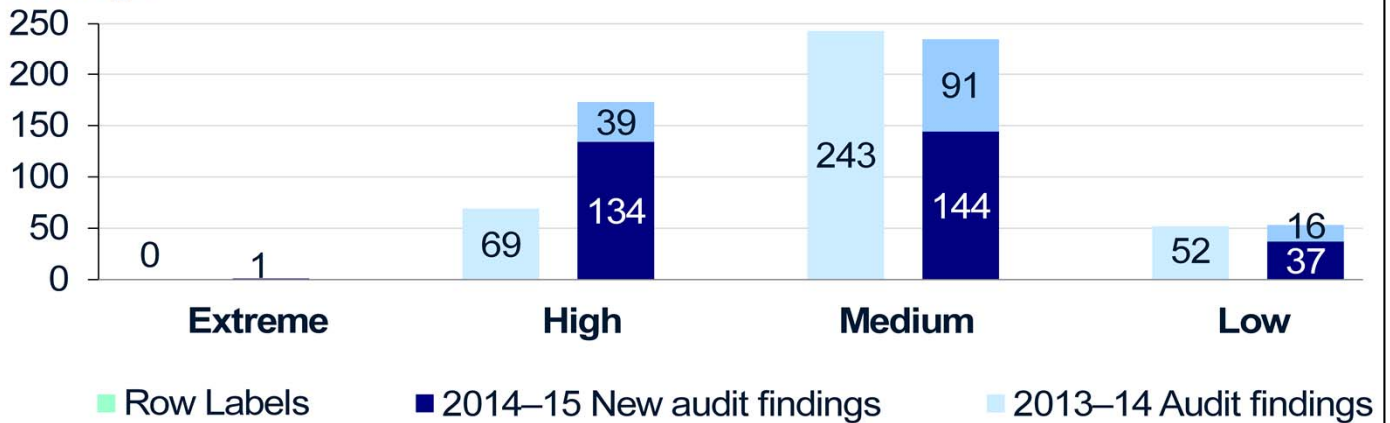
41 percent of prior-period IT audit findings have not been remediated, many of which were rated high risk.

More focused attention and oversight by accountable officers and governance bodies is required to address our IT audit findings.

## Results of IT audits – *continued*

High risk audit findings increased from 69 in financial year 2013–14 to 134 in the current year.

### Findings



Medium- and low-risk findings have remained relatively stable with the biggest increase being high-risk issues, from 69 high-risk audit findings identified in financial year 2013–14 to 134 high-risk audit findings in the current year.

In one of our audited entities, we reported an extreme-risk audit finding. This entity was found to have password management policies and configurations which are not consistent with Victorian Government IT standards.



## Results of IT audits – *continued*

pages  
19–36

Of the 134 high-risk IT audit findings, 91% relate to:

- managing access and authenticating users to IT applications and data
- assurance obtained by entities over IT general controls performed by external organisations
- entities using IT systems, which are no longer, or soon not to be, supported by vendors.

No formalised framework in place at the whole-of-Victorian-Government level which prioritises IT systems recovery.

**Consistent with previous years, a significant number of IT audit findings relate to IT security.**

Consistent with previous years, a significant number of IT audit findings relate to IT security.

91 per cent of all high-risk IT audit findings are concentrated around the following IT general controls categories:

- managing access and authenticating users to IT applications and data
- assurance obtained by entities over IT general controls performed by external organisations
- entities using IT systems which are no longer supported by vendors.

There continues to be no formalised framework in place at the whole-of-Victorian-government level which prioritises IT systems recovery in the event of a disaster impacting a number of departments and agencies.

## Focus areas 2014–15

10

pages  
49–60

Identity and access management controls at more than half of the 30 in-scope entities require improvement.

- Improvements required to user access management, ongoing monitoring and authentication methods, such as passwords.

Software licensing is generally well managed across the in-scope entities.

- Improvements required to software licensing policies and procedures and compliance monitoring.

Our 2014–15 areas of focus were identity and access management and software licensing. 30 entities were in-scope for this review.

Identity and access management controls at more than half of the 30 in-scope entities require improvement. Improvement areas mostly relate to user access management, ongoing monitoring and authentication methods, such as passwords.

Software licensing is generally well-managed across the in-scope entities, however, a number of improvement opportunities were noted. Improvement areas mostly relate to software licensing policies and procedures and compliance monitoring.

## Recommendations

11

		Accept
That the Commissioner for Privacy and Data Protection:		
1.	provides education and training to relevant entities on the requirements of the Victorian Protective Data Security Standards—once issued.	✓
That the Department of Premier & Cabinet:		
2.	monitors and reports the status of information technology obsolescence risks at departments and public sector agencies	✓
8.	monitors and reports the status of the implementation of disaster recovery frameworks and plans by shared services boards.	✓

This audit made 10 recommendations. All recommendations have been accepted.

One recommendation has been directed to the Commissioner for Privacy and Data Protection and two recommendations have been directed to the Department of Premier and Cabinet.

## Recommendations – *continued*

12

Accept

That public sector entities' governing bodies and management:

- |    |  |   |
|----|--|---|
| 3. | enhance management's understanding of their <i>Financial Management Act 1994</i> and Standing Directions obligations, and ensure: <ul style="list-style-type: none"> <li>• assurance reports received for outsourced information technology environments are reliable and fit-for-purpose</li> <li>• exceptions raised in assurance reports are assessed for the impact they may have on the entity's control environment</li> </ul> | ✓ |
| 4. | manage the continuity of vendor support for systems approaching end-of-life, including its upgrade or migration to fully supported solutions. Where possible, entities should work collaboratively to address information technology obsolescence risk across the public sector.   | ✓ |

Seven recommendations have been directed to all public sector entities.

## Recommendations – *continued*

13

Accept

That public sector entities' governing bodies and management:

- |    |   |   |
|----|---|---|
| 5. | implement appropriate governance and monitoring mechanisms to ensure: <ul style="list-style-type: none"> <li>• information technology audit findings are addressed by management</li> <li>• sustainable process improvements, to prevent future recurrence</li> </ul> | ✓ |
| 6. | align information technology control frameworks to relevant Victorian Government information technology security standards.   | ✓ |



## Recommendations – *continued*

14

		Accept
That public sector entities' governing bodies and management:		
7.	ensure that, where relevant, shared service providers implement disaster recovery frameworks which prioritise information technology systems recovery in the event of a disaster impacting a number of departments and agencies. The framework and plans should cover financial and non-financial systems	✓
9.	enhance identity and access management, and software licensing policies and procedures by addressing control weaknesses reported in management letters	✓
10.	implement processes to periodically monitor the effectiveness of identity and access management, and software licensing processes and controls.	✓

## Key messages

15

**For the 2014–15 financial year, there are three clear emerging themes:**

- The management of controls at outsourced IT environments requires attention.
- The use of IT systems that are at their end-of-life needs to be addressed.
- IT security controls need improvement.

**More focused attention and oversight by accountable officers and governance bodies is required to address our IT audit findings.**

**Consistent with previous years, a significant number of IT audit findings relate to IT security.**

To recap the key messages from the audit are:

- For the 2014–15 financial year, there are three clear emerging themes.
  - The management of controls at outsourced IT environments requires attention.
  - The use of IT systems that are at their end-of-life needs to be addressed.
  - IT security controls need improvement.
- More focused attention and oversight by accountable officers and governance bodies is required to address our IT audit findings.
- Consistent with previous years, a significant number of IT audit findings relate to IT security.

## Overall message

16

**Our financial audits continue to identify a large number of IT control deficiencies, which have the potential to impact the confidentiality, integrity and availability of public sector financial data and IT systems.**

The overall message of the audit is:

- Our financial audits continue to identify a large number of IT control deficiencies, which have the potential to impact the confidentiality, integrity and availability of public sector financial data and IT systems.
- In the coming months VAGO will publish a better practice guide to enhance the IT control environment at public sector entities.

## Relevant audits

- *Delivering Services to Citizens and Consumers via Devices of Personal Choice: Phase 2 (2015)*
- *Delivering Services to Citizens and Consumers via Devices of Personal Choice: Phase 1 – Interim Report (2015)*
- *Digital Dashboard: Status Review of ICT Projects and Initiatives (2015)*
- *Information and Communications Technology Controls Report 2013–14 (2014)*

There are four relevant previously published audits:

- *Delivering Services to Citizens and Consumers via Devices of Personal Choice: Phase 2 (2015)*
- *Delivering Services to Citizens and Consumers via Devices of Personal Choice: Phase 1 – Interim Report (2015)*
- *Digital Dashboard: Status Review of ICT Projects and Initiatives (2015)*
- *Information and Communications Technology Controls Report 2013–14 (2014)*

## Contact details

18

For further information on this presentation please contact:

Victorian Auditor-General's Office

[p] 8601 7000

[w] [www.audit.vic.gov.au/contact\\_us.aspx](http://www.audit.vic.gov.au/contact_us.aspx)

All our reports are available on our website.

If you have any questions about this or other reports, or if you have anything else you would like to discuss with us including ideas for future audit topics, please call us on 03 8601 7000 or contact us via our website.