Financial Systems Controls Report: Information Technology 2014–15

Victorian Auditor-General's Report | October 2015 | 2015–16:10

VICTORIA

Victorian
Auditor-General

Financial Systems Controls Report: Information Technology 2014–15

Ordered to be published

VICTORIAN
GOVERNMENT PRINTER
October 2015

PP No 98, Session 2014–15

This report is printed on Monza Recycled paper. Monza Recycled is certified Carbon Neutral by The Carbon Reduction Institute (CRI) in accordance with the global Greenhouse Gas Protocol and ISO 14040 framework. The Lifecycle Analysis (LCA) for Monza Recycled is cradle to grave including Scopes 1, 2 and 3. It has FSC Mix Certification combined with 55% recycled content.

ISBN 978 1 925226 36 2

VAGO
Victorian Auditor-General's Office
Auditing in the Public Interest

The Hon. Bruce Atkinson MLC
President
Legislative Council
Parliament House
Melbourne

The Hon. Telmo Languiller MP
Speaker
Legislative Assembly
Parliament House
Melbourne

Dear Presiding Officers

Under the provisions of section 16AB of the *Audit Act 1994*, I transmit the *Financial Systems Controls Report: Information Technology 2014–15*.

This report builds on VAGO's previous inaugural *Information and Communications Technology Controls Report 2013–14* and aims to provide additional insight and increased visibility of IT related audit findings. The report is intended to provide decision-makers with relevant information to help them address IT audit findings and improve processes and controls.

For this audit, 45 entities with a financial year-end date of either 31 December 2014 or 30 June 2015 were selected for analysis. Sixty-five key financial IT applications and their infrastructure were audited, with 462 associated audit findings used as the basis for this report's analysis. Additionally, we have performed maturity assessments of selected entities' IT environments and examined two focus areas—identity and access management, and software licensing.

Most of our IT audit findings were rated medium and high risk, with one audit finding rated as an extreme risk. Along with the specific IT audit findings, this report also draws out three clear emerging themes.

The recommendations aim to assist public sector agencies address the identified IT audit findings and improve their IT control environments.

As part of our work this financial year, we have provided an update on the prior year high-level recommendations made as part of the *Information and Communications Technology Controls Report 2013–14*.

Yours faithfully

Dr Peter Frost
Acting Auditor-General

7 October 2015

Contents

Auditor-General's comments

Each financial year VAGO undertakes a number of information technology (IT) audits to verify whether key financial systems are managed appropriately to support financial reporting process.

A total of 462 IT audit findings were found at the 45 entities selected for this report. Similar to last year, management at these entities continue to be slow to act on our findings, especially our high-risk findings. This demonstrates the need for more focused attention and oversight of IT issues by accountable officers and governance bodies, including audit committees. As a result, we intend to increase the level of accountability over the recommendations that are raised with management, especially at those entities that are not addressing our findings adequately or on a timely basis.

While there have been positive developments in the governance of outsourced IT arrangements, more effort is required by entities to enhance their visibility and accountability over outsourced activities and to assess the impact these activities have on entities' control environments. This year, inadequacies in assessing the reliability and quality of the audits conducted over their outsourced IT environments led to delays in finalising the financial reports of a number of entities, as well as additional audit costs and delays in finalising this report.

Alarmingly, each year VAGO is finding a large number of IT systems and software which are either no longer supported or fast approaching the end of support by the vendor. This poses IT security and operational risks to the entities IT environment, as well as unnecessary added costs.

Disappointingly, IT security-related audit findings continue to be raised and again account for the majority of our audit findings. It is also disappointing that our recommendation for a whole-of-government disaster recovery framework has not been addressed since it was first made in 2012–13.

This year we analysed two areas of focus—identity and access management, and software licensing. While software licensing was generally well controlled, controls to reduce the risk of inappropriate access to IT systems require significant improvement.

We have previously raised concerns regarding the Auditor-General's outdated mandate which restricts examination of public sector services undertaken by the private sector. These concerns continue and in the current year, VAGO was explicitly denied audit access by a private sector IT service provider. Consequently VAGO was unable to complete an audit of a public sector entity's IT environment and was forced to adopt a less efficient and more costly audit approach.

Audit team

Karen Phillips
Engagement Leader

Ian Yaw
Team Leader

Tonderai Nduru
Team Member

Engagement Quality Control Reviewer

Paul Martin

In the coming months VAGO will publish a better practice guide to enhance the IT control environment at public sector entities. I encourage all public sector entities to assess their IT control environment against this better practice guide.

Dr. Peter Frost
Acting Auditor-General

October 2015

Audit summary

This report summarises the results of our audits of selected public sector entities' information technology (IT) controls, performed in support of VAGO's 2014–15 financial audits. This report also summarises our reviews of two focus areas—identity and access management (IDAM), and software licensing practices.

IT controls are policies, procedures and activities put in place by an entity to assist and maintain the confidentiality, integrity and availability of its IT systems and data. IDAM consists of frameworks, policies and practices established to reduce the risk of inappropriate access to information systems and data. Software licensing controls are policies and practices implemented to manage the procurement and deployment of software, as well as ongoing compliance with vendor agreements.

This report is in its second year and builds on the inaugural *Information and Communications Technology Controls Report 2013–14* to provide additional insight and to aggregate our IT audit findings. This report is also intended to provide decision-makers with relevant information to assist them to address IT audit findings, improve processes and controls, and to enhance accountability across the public sector.

For this audit, 45 entities with a financial year-end date of either 31 December 2014 or 30 June 2015 were selected for analysis. The audit findings relating to 65 IT applications relevant to financial reporting and associated IT infrastructure are analysed in this report.

The audit findings give a high-level view of IT general controls and weaknesses, and identify broad trends that may not be covered in reports we make to an entity's management during the course of a financial audit.

Conclusions

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 IT audit findings identified were rated medium and high risk, with one rated as an extreme risk. Notably, the number of high-risk audit findings increased from 69 in 2013–14 to 134 in 2014–15. The key reason for this significant increase is related to IT security and the risks associated with using IT systems that are past or approaching their end-of-life. These were two of the three themes identified this year.

More focused attention and oversight by accountable officers and governance bodies is required to address our IT audit findings from previous years and to ensure sustainable process improvements are implemented to prevent future recurrence. Forty-one percent of our IT audit findings from previous years have not been addressed, many of which were rated high-risk.

Despite the identified IT control deficiencies, entity's control environments were reliable for financial reporting purposes, as satisfactory mitigations were in place, such as compensating management controls or alternative audit procedures.

For the 2014–15 financial year, there are three clear emerging themes. These are detailed in our Findings.

Findings

The three themes identified by our 2014–15 IT audits:

- **The management of controls at outsourced IT environments requires attention**—outsourced IT environments are in place for a number of in-scope entities, with the state's IT shared services body, CenITex, being such an example. While there have been overall improvements during the year in how outsourced IT environments are managed, additional improvements are still required. There is a need to increase awareness of ownership and obligations relating to these outsourced environments, including assessing the reliability and quality of audits conducted over an entity's outsourced environment and assessing the impact of any control weaknesses on the entities' control environment. Contracts with service providers should not limit the ability of the entity to review the outsource providers' controls environment.
- **The use of IT systems that are at their end-of-life needs to be addressed**—some of the software used to support financial systems are nearing their end-of-support dates or are past the support dates, and may result in increased risks and maintenance costs to in-scope entities.
- **IT security controls need improvement**—IT security control weaknesses account for 68 per cent of all IT audit findings. There is poor management of IT security, particularly relating to user access and alignment with Victorian Government IT security standards.

A total of 462 IT audit findings were reported. Of the 134 high-risk IT audit findings, 91 per cent relate to:

- managing access to IT applications and data
- authenticating users to IT systems, such as password controls
- 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.

Recommendations

Number	Recommendation	Page
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.	17
That the Department of Premier & Cabinet:		
2.	monitors and reports the status of information technology obsolescence risks at departments and public sector agencies	17
8.	monitors and reports the status of the implementation of disaster recovery frameworks and plans by shared services boards. These frameworks and plans should: • prioritise information technology systems recovery in the event of a disaster impacting a number of departments and agencies • cover financial and non-financial systems.	48
That public sector entities' governing bodies and management:		
3.	enhance management's understanding of their *Financial Management Act 1994* and Standing Directions obligations, and ensure: • assurance reports received for outsourced information technology environments are reliable and fit-for-purpose • exceptions raised in assurance reports are assessed for the impact they may have on the entity's control environment	17
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	18
5.	implement appropriate governance and monitoring mechanisms to ensure: • information technology audit findings are addressed by management • sustainable process improvements, to prevent future recurrence	18
6.	align information technology control frameworks to relevant Victorian Government information technology security standards.	18

Recommendations – *continued*

Number	Recommendation	Page
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	48
9.	enhance identity and access management, and software licensing policies and procedures by addressing control weaknesses reported in management letters	60
10.	implement processes to periodically monitor the effectiveness of identity and access management, and software licensing processes and controls.	60

Submissions and comments received

We have engaged with the Deputy Secretary, Governance Policy and Coordination within the Department of Premier & Cabinet, the Commissioner for Privacy and Data Protection, the Deputy Secretaries of the portfolio departments and the Chief Information Officer Council throughout the course of the audit. In accordance with section 16(3) of the *Audit Act 1994*, we provided a copy of this report to the audited agencies and requested their submissions or comments.

We have considered those views in reaching our audit conclusions and have represented them to the extent relevant and warranted. The full section 16(3) submissions and comments are included in Appendix C.

1 Background

1.1 Introduction

When planning a financial audit, VAGO seeks to understand and evaluate an entity's information technology (IT) environment and any related risks to the reliability of financial reporting.

This report summarises the results of this work on selected public sector entities' IT general controls as part of the 2014–15 financial audits. This is the second report of its kind and aims to provide extra insight into VAGO's IT audit findings, and identify wider trends that may not be covered in reports to an entity's management.

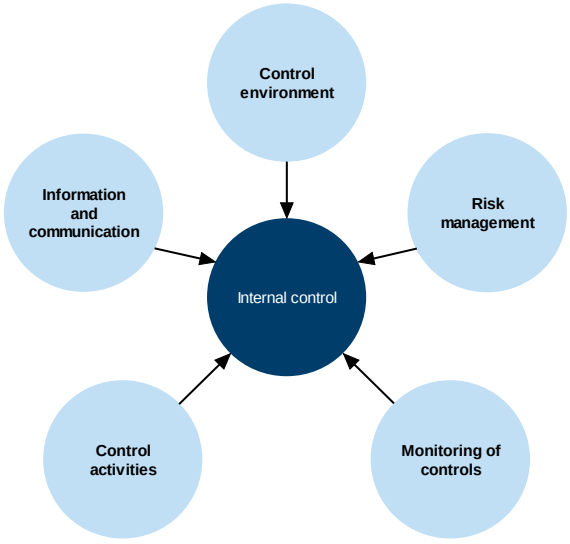
The report also summarises the outcomes of reviews performed over the focus areas of identity and access management, and software licensing.

1.2 Internal control framework

An entity's governing body and its accountable officer are responsible for developing and maintaining an internal control framework. Internal controls are systems, policies and procedures which help an entity to reliably and cost effectively meet its objectives, as well as minimise risk and fraud.

The components of an internal control framework are shown in Figure 1A.

Figure 1A
Components of an internal control framework



Source: Victorian Auditor-General's Office.

In Figure 1A:

- **Control environment**—provides the fundamental discipline and structure for controls and includes governance and management functions as well as the attitudes, awareness and actions of those charged with governance and management of an entity.
- **Risk management**—involves identifying, analysing, mitigating and controlling risks.
- **Monitoring of controls**—involves observing the internal controls in practice and assessing their effectiveness.
- **Control activities**—policies, procedures and practices issued by management to help meet an entity's objectives.
- **Information and communication**—involves communicating control responsibilities throughout the entity and providing information in a form and time frame that allows staff to discharge their responsibility.

An annual financial audit enables the Auditor-General to form an opinion on an entity's financial report. An integral part of this process, as well as a requirement of Australian Auditing Standard ASA 315 *Identifying and Assessing the Risk of Material Misstatement through Understanding the Entity and its Environment,* is to evaluate the strengths of an entity's internal control framework and governance processes as they relate to its financial reporting.

While the auditor considers the internal controls relevant to financial reporting, there is no requirement for the auditor to provide an opinion on their effectiveness. Consequently, an unmodified audit opinion on the financial report is not an opinion on the adequacy or otherwise of the entity's internal control environment as any control inadequacies are mitigated by additional audit work. The ultimate responsibility for the effective operation of the internal control at all times remains with the entity's management.

Significant internal control deficiencies identified during an audit are communicated to the entity's governing body and management so that they may be rectified in the management letter. Such deficiencies or weaknesses in controls will usually not result in a qualified audit opinion as often an entity will have compensating controls in place that aid in mitigating the risk of a material error or misstatement in the financial report, or the auditor may be able to obtain evidence through performing substantive procedures.

However, for entities that use highly automated IT systems to initiate and process financial transactions, the IT system is the sole repository of the record of transactions. A significant internal control weakness in the IT system may result in a qualification if it prevents the auditor from obtaining sufficient evidence about the accuracy, completeness and reliability of the financial information being reported.

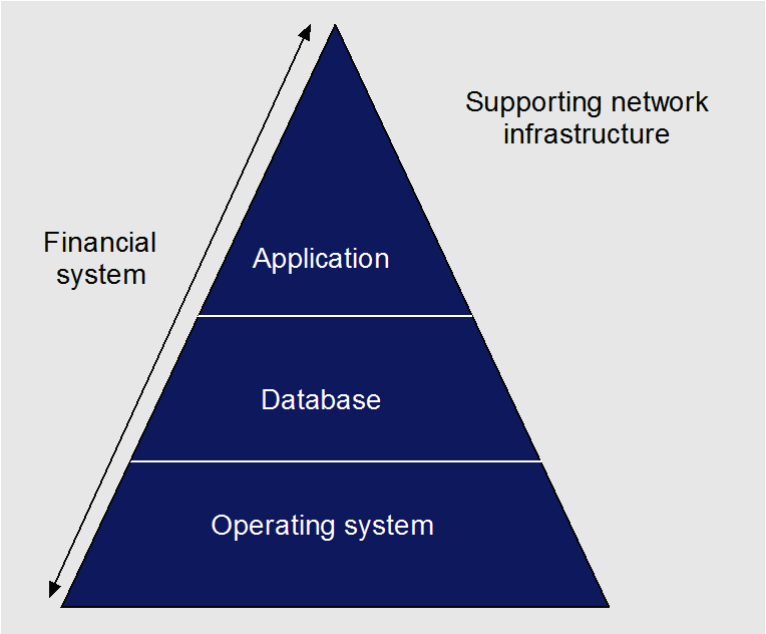
1.2.1 The importance of IT systems and IT general controls

An IT system is a collection of computer hardware and programs that work together to support business or operational processes. IT systems are generally made up of three components:

- **Operating system**—core programs that run on the IT hardware that enable other programs to work. Examples of operating systems include Microsoft Windows, Unix and IBM OS/400.
- **Databases**—programs that organise and store data. Examples of database software include an Oracle database and Microsoft SQL Server.
- **Applications**—programs that deliver operational or business requirements. There are various types of IT applications, which are described in Section 1.5.

These components are supported by an entity's network infrastructure. A typical VAGO scope for an IT general controls audit covers all three IT system components for in-scope key financial systems. This is shown in Figure 1B.

Figure 1B
Typical scope for an IT general controls audit



Source: Victorian Auditor-General's Office.

IT general controls are policies, procedures and activities put in place by an entity to assist and ensure the confidentiality, integrity and availability of its IT systems and data.

Auditing Standard ASA 315 *Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment* states that IT benefits internal control by enabling an entity to:

- consistently apply predefined business rules and perform complex calculations in processing large volumes of transactions or data
- enhance the timeliness, availability, and accuracy of information
- reduce the risk that controls will be circumvented
- enhance the ability to achieve effective segregation of duties by implementing security controls in applications, databases, and operating systems.

An example of an IT general control is whether access requests to IT systems are properly reviewed and authorised by management. The objective of this control is to ensure only authorised users have access to the entities' IT systems.

Ineffective IT general controls may have an impact on the reliability and integrity of the system's underlying financial data and programs and may impact the ability of VAGO to rely on underlying business and process controls.

Auditing Standard ASA 265 *Communicating Deficiencies in Internal Control to Those Charged with Governance and Management* requires the auditor to:

- communicate, in writing, all significant deficiencies in internal control and their potential effects to those charged with governance, and where appropriate, management
- communicate to management other identified deficiencies in internal control that the auditor considers to be of sufficient importance to merit management's attention.

Weaknesses identified by VAGO during an IT audit are brought to the attention of the entity's accountable officer and chair of the governing body, as well as the chief financial officer, chief information officer and audit committee, by way of a management letter. We also seek management's comments on remediation plans and time frames for addressing any audit observations or recommendations.

1.3 Recent key changes to the sector

Recent changes within the public sector have impacted the scope of our IT audits.

1.3.1 Machinery-of-government changes

Following the Victorian state election on 29 November 2014 and the formation of a new state government, machinery-of-government changes were made in January 2015 to restructure key departments and agencies.

From an IT perspective, most notable was the transition of responsibilities for whole-of-Victorian-Government (WoVG) IT strategy, policy, and operations from the former Department of State Development, Business & Innovation (DSDBI) to the Department of Premier & Cabinet (DPC).

There were several other impacts:

- The governance and leadership roles of Minister for Technology and Chief Technology Advocate were abolished.
- Following the transition of the whole-of-public-sector IT portfolio to DPC, the Digital Government Branch was renamed the Enterprise Solutions Branch and its coverage includes:
  - **WoVG Projects Reporting Assurance**—coordinates briefs, audit responses, correspondence and other content for the branch.
  - **Business Systems, Policy and Standards**—defines standards for the procurement of new business systems, plus WoVG policies for IT and business systems. Also responsible for the development of the WoVG IT strategy.
  - **Shared Services Governance and Assurance**—develops the governance framework for shared services operations and provides progress reports on the implementation of the shared services agenda.

VAGO consulted with DPC as the lead agency for this report.

1.3.2 CenITex

CenITex is an IT shared services agency, set up as a state body by the Victorian Government in July 2008 to centralise IT services for government agencies.

As a key service provider of IT services to a number of government departments and agencies, a number of this audit's findings are associated with CenITex, and the IT infrastructure and processes that it manages.

In recent years, there have been uncertainties over CenITex's future with a number of projects initiated to evaluate potential options, including outsourcing to the private sector.

On 30 June 2015, the government announced that it would implement a new approach to the establishment and management of shared business support services. The announcement also clarified that CenITex would continue to provide IT services that are specific to government and that the other services provided by CenITex, that are readily available in the market, would be market tested over the next year.

It should be noted that work performed as part of our financial audits does not assess the effectiveness or efficiency of CenITex.

1.3.3 Commissioner for Privacy and Data Protection

The *Privacy and Data Protection Act 2014* came into effect on 17 September 2014. This legislation significantly changes the regulatory landscape for privacy and data protection in the Victorian public sector.

The Act sets out three main areas of focus:

- Part 1: Information Privacy
- Part 2: Data Protection
- Part 3: Law Enforcement Data.

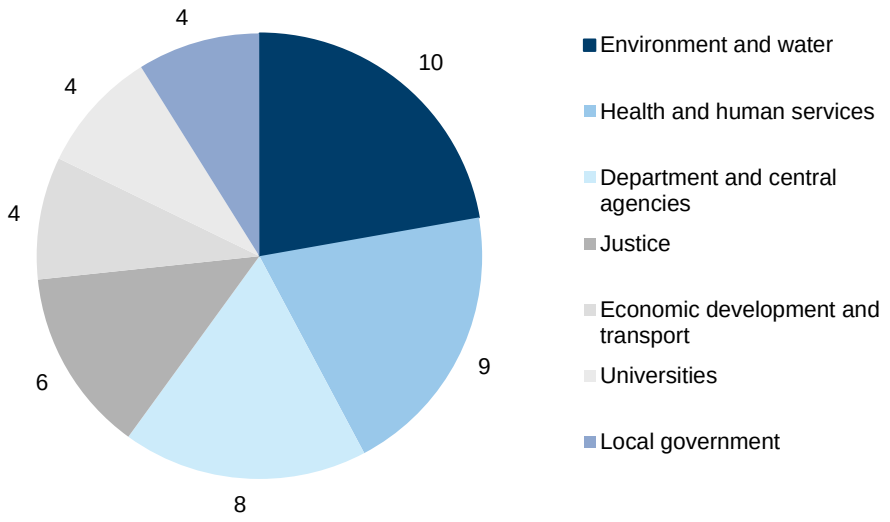
In July 2015, the draft Victorian Protective Data Security Standards were released for stakeholders comments. Given the significant role of the Commissioner, VAGO will monitor standards and guidelines issued by the Commissioner and the impact on IT control requirements across government.

1.4 Departments and agencies in scope

This report summarises the results of the audits of IT general controls conducted as part of the annual financial audits of 45 selected entities, with a financial year-end date of either 31 December 2014 or 30 June 2015—the audited agencies are listed in Appendix B.

The selected entities are summarised by sector in Figure 1C.

Figure 1C
Selected in-scope entities by sector



Note: For the purposes of this report, departments are grouped with central agencies.
Source: Victorian Auditor-General's Office.

The most represented sectors are:

- environment and water—10 entities
- health and human services—nine entities
- department and central agencies—eight entities
- justice—six entities.

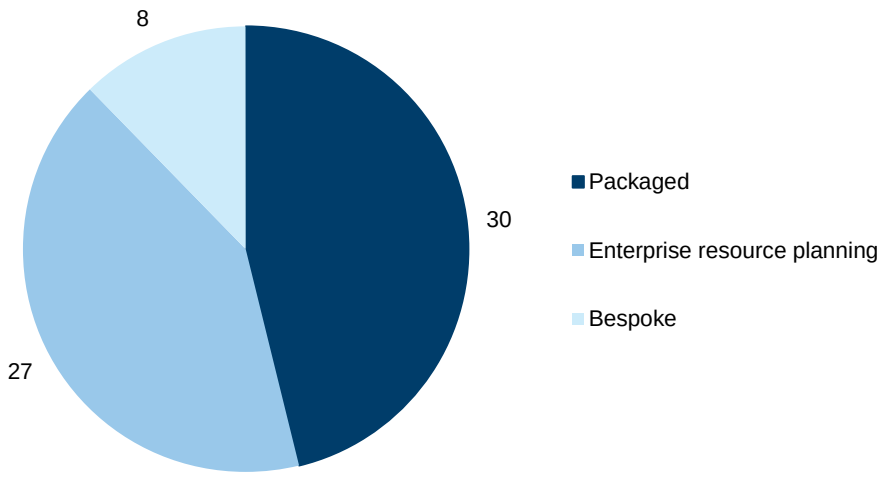
This report will largely focus on these four sectors, which represent about 74 per cent of our in-scope entities. The characteristics of the entities within these sectors are found in Part 3.5.

1.5 IT systems in scope

Within the 45 selected entities, we audited IT general controls relating to 65 IT applications and associated IT infrastructure. These applications are a combination of financial and operational applications that support key financial processes.

The types of IT applications in scope are summarised in Figure 1D.

Figure 1D
In-scope IT applications by type



Source: Victorian Auditor-General's Office.

A description of the IT applications follows:

- **Bespoke software**—includes custom developed applications that are purpose built with a specific need in mind, e.g. the myki system used by Public Transport Victoria.
- **Enterprise Resource Planning**—complex applications that deliver a wide range of business processes across the organisation. For example, the Oracle E-business suite is used to support financial reporting in a number of departments and agencies.
- **Packaged applications**—also known as commercial 'off-the-shelf' packages, are usually designed to support a specific process. This software will typically function without extensive customisation, although there have been some instances of customisation. For example, the Chris21 application is used to support payroll processes in a number of entities.

1.6 Reliance on the work of others

To reduce duplication of audit effort and to maximise audit effectiveness and efficiency, as part of VAGO's audit methodology, the audit team considered the work performed by other parties where a similar scope of work was performed during the audit period.

From an IT perspective, reliance on work performed by others can be grouped into two categories:

- **Internal audit**—an effective internal audit function will often allow a modification in the nature and timing, and a reduction in the extent of procedures performed by VAGO, but cannot entirely eliminate the need for independent testing. When we intend to rely on specific internal audit work, we evaluate and test that work to confirm its adequacy for our purposes.
- **Service assurance reports**—these reports typically relate to shared service providers for IT or data processing services and external investment managers. CenITex is an example of such an arrangement. Where such organisations are used to support controls over key processes, we seek to obtain a service assurance report that describes the control environment. These reports provide independent assurance to management that an effective internal control environment had been maintained, which allows them to meet the requirements under the provisions of the *Financial Management Act 1994* pursuant to the Standing Directions of the Minister for Finance.

Where the work of others can be used to support our audit testing of IT processes and controls, VAGO assesses the scope and findings for impact on our financial audit approach. This would, in turn, guide any additional testing that may be required.

For the purposes of this report, where VAGO has relied on the work of others in our financial audits, relevant findings identified by the service auditor have been consolidated with our work.

1.7 Audit conduct

The audits of the 45 entities were undertaken in accordance with Australian Auditing Standards. Pursuant to section 20(3) of the *Audit Act 1994*, unless otherwise indicated, any persons named in this report are not the subject of adverse comment or opinion.

The cost of preparing and printing this report was $215 000.

1.8 Structure of the report

The remainder of this report is structured as follows:

- Part 2 examines the top three themes or trends noted during the course of the IT audits
- Part 3 provides a summary of the IT audit findings noted as part of the 2014–15 audits and an IT general controls maturity assessment conducted by VAGO
- Part 4 examines the two focus areas—identity and access management, and software licensing.

2 Themes from IT audits

At a glance

Background

Key information technology (IT) audit themes are drawn from testing performed as part of each entity's annual financial audit, as well as discussions with management and analysis of our IT audit findings. These themes are prepared to provide insight and actionable recommendations for public sector entities.

Conclusion

For the 2014–15 financial year, we identified three clear emerging themes from IT audits, and have made a number of recommendations to address them.

Findings

- The management and oversight of IT controls by external service providers requires improvement.
- Entities are continuing to use IT applications and systems that are approaching the end of the vendor's support cycle.
- A large number of our IT audit findings relate to IT security control weaknesses.

Recommendations

- That the Commissioner for Privacy and Data Protection provides education and training to relevant entities on the requirements of the Victorian Protective Data Security Standards—once issued.
- That Department of Premier & Cabinet monitors and reports the status of information technology obsolescence risks at departments and public sector agencies.
- That public sector entities' governing bodies and management:
  - enhance management's understanding of their *Financial Management Act 1994* and Standing Directions obligations
  - manage the continuity of vendor support for systems approaching end-of-life
  - implement appropriate governance and monitoring mechanisms to ensure IT audit findings are addressed by management to prevent future recurrence
  - align IT control frameworks to relevant Victorian Government IT security standards.

2.1 Introduction

This Part discusses:

- the top three themes noted during the information technology (IT) audits conducted for the 2014–15 financial year
- the root cause analysis and insights into the IT audit themes
- the strategic implications and recommendations for possible future action plans.

2.2 Top three themes noted in 2014–15

Based on our analysis of the IT audit findings noted during 2014–15, there were three top themes:

- **The management of controls at outsourced IT environments requires attention**—the management and oversight of IT controls undertaken by external service providers requires improved governance and oversight.
- **The use of IT systems that are at their end-of-life needs to be addressed**—entities are continuing to use IT applications and systems that are approaching the end of the vendor's support cycle.
- **IT security controls need improvement**—a large number of our IT audit findings relate to IT security control weaknesses.

2.2.1 Management of controls at outsourced IT environments

Our observations

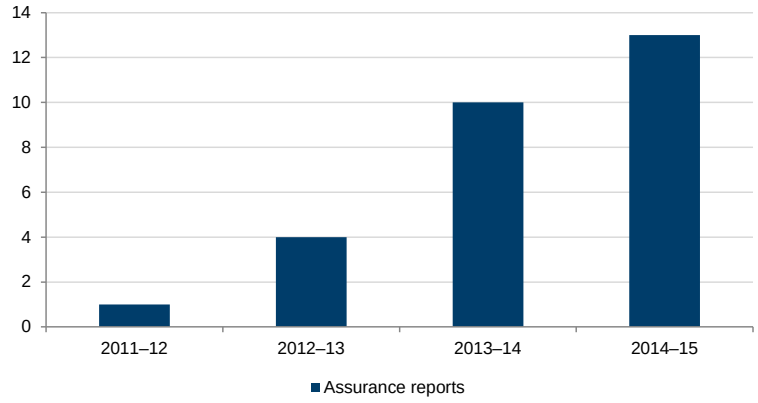
When a public sector entity relies on an outsourced provider or 'cloud' service providers to operate and maintain their IT environment, management needs to obtain assurance that the controls implemented and managed by the outsourced provider are operating effectively. Typically, cloud service providers provide their services to the organisation—in the form of software, infrastructure and platform—over the Internet. By using an outsourced IT arrangement, the entity's management does not forego its duty to ensure that controls are adequate and that the entity's data and information is protected.

The effectiveness of controls at these outsourced IT environments is typically reported to a public sector entity through a service assurance report such as *ASAE 3402 Assurance Reports on Controls at a Service Organisation* or *AUS 810 Special Purpose Reports on the Effectiveness of Control Procedures*. Public sector entities need to request that the outsourced IT provider engage an auditor to perform this work and report back to them. This enables entities to certify their annual financial report and complete the Standing Directions of the Minister for Finance certification.

Consistent with the inaugural *Information and Communication's Technology Controls Report 2013–14* (ICT Controls Report 2013–14), there continues to be a noticeable upward trend in the number of service assurance reports being obtained by public sector entities. These reports are relied upon by the public sector entity for attesting to the overall strength of the external providers controls environment and are relied upon by VAGO for our financial audits.

In 2014–15, 13 assurance reports for the IT general controls at outsourced IT environments were provided to VAGO. This compares to 10 in 2013–14, four in 2012–13 and one in 2011–12. This trend is shown in Figure 2A.

Figure 2A
Number of assurance reports relied upon by VAGO for financial audits



Note: Where multiple service assurance reports are prepared for a shared service IT provider such as CenITex, this is counted as one report.
Source: Victorian Auditor-General's Office.

For 2014–15, VAGO actively discussed the control weaknesses identified in these reports with management and audit committees. As part of their obligations of maintaining a sound control environment, VAGO has encouraged management to review these assurance reports with greater rigour and to acquit and take ownership over the weaknesses.

As part of this and as committed to in last year's ICT Controls Report 2013–14, VAGO has commenced reporting on relevant weaknesses arising from assurance reports with the aim of:

- improving overall accountability
- driving the tracking of these weaknesses by management and audit committees
- enhancing remediation of the weaknesses.

Insights and implications

Since first highlighting this theme in the ICT Controls Report 2013–14, there have been some notable changes.

Policy guidance

The *Financial Management Act 1994* and the Standing Directions of the Minister for Finance require an entity's management to maintain an effective internal controls environment.

In our ICT Controls Report 2013–14, we recommended that further policy guidance was required at the whole-of-government level, as a number of agencies did not currently obtain any form of assurance over outsourced controls. During 2014–15, VAGO consulted with the Department of Treasury & Finance (DTF) which led to the publishing of the *Key advice update No 1, 2015 - Managing outsourced financial services* to provide further guidance to entities utilising such arrangements. Guidance specific to managing outsourced IT arrangements is not available.

Improved management accountability

As described in our ICT Controls Report 2013–14, there was a perception among some public sector entities that in an outsourcing arrangement the risks associated with the control environment are also transferred, which is not the case. In our interactions with the management of those entities this year, there has been a growing awareness and acceptance of management's responsibilities. This has directly resulted in an increase in the number of service assurance reports received, or other instruments used to obtain assurance.

Worryingly, there remain pockets of limited awareness and acceptance, including high-risk entities, of the risks and responsibilities associated with outsourced arrangements. As a result we will continue to encourage a culture of ownership and responsibility across the public sector.

While there has been a marked improvement in available policy guidance and management accountability over service organisation assurance, these areas still require improvement.

Access to review controls at private sector entities

The current *Audit Act 1994* limits the Auditor-General's ability to directly follow up on the activities and controls of private sector entities, which are increasingly delivering cloud services and outsourced arrangements to the public sector. The Audit Act's limitations have been a recurring concern, and during 2014–15 VAGO was explicitly denied audit access by a private sector service provider. Figure 2B highlights why there is an urgent need to amend the *Audit Act 1994*.

Figure 2B
Case study: *Audit Act 1994* limitations

During the 2014–15 audit of a public sector entity, the entity's payroll process was evaluated to be material to the financial report. The entity's payroll process utilised a cloud-based application ('software-as-a-service').
The cloud-based application vendor had not provided the public sector entity with an assurance report and there was no 'right of audit' embedded within the contract between the entity and the vendor. Management similarly did not have any visibility over most of the controls implemented by the vendor.
While the vendor was willing to provide a portion of the information requested to enable VAGO to undertake the audit, key audit evidence, such users access listings to the entity's data, was deemed by the vendor to be commercial-in-confidence, or too sensitive to be released.
Because of the current mandate limitation, we were unable to access the information required to assess the operating efficiency of the controls that prevent and detect payroll errors from occurring. As a result, VAGO was unable to complete an audit of the IT environment and a less efficient approach was undertaken, resulting in unnecessary higher audit costs.
This issue was raised in our management letter as management does not have visibility over, and has not received assurance over, controls operating in this outsourced IT environment as required by the *Financial Management Act 1994*.

Source: Victorian Auditor-General's Office.

Entities review of the reliability and results of assurance reports

To ensure entities are meeting their obligations under the *Financial Management Act 1994*, an increased emphasis is needed on assessing the reliability of assurance reports and understanding the impact the issues raised may have on their control environment. Figure 2C details a case study where greater rigour over an assurance report was required during 2014–15.

Figure 2C
Case study: CenITex Service Assurance Program

CenITex is a key provider of IT services to a number of in-scope departments and agencies. In addition to the operational activities that it delivers, CenITex also coordinates and manages a service assurance program, which aims to deliver assurance reports prepared in accordance with auditing or assurance standards, dependent on the department or agencies requirements.
During 2014–15 VAGO raised concerns about the quality and reliability of these assurance reports. As a result, we did not place full reliance on these assurance reports and for the purposes of our 2014–15 financial audits, we conducted independent audit testing. This led to delays in finalising the financial reports of the affected departments and agencies, as well as additional audit costs and a delay in finalising this report.
Concerns over the reliability of the assurance reports also led to concerns about whether departments and agencies had sufficiently met their obligations under the *Financial Management Act 1994*. VAGO requested that management at the departments and agencies undertake additional procedures to assess the overall operation of IT controls, including the reliability of the assurance reports, their findings and any control areas not assessed by the CenITex auditor.
This finding was raised in our management letters to the relevant departments and agencies as these entities have not implemented a sustainable process to ensure that management assesses the reliability of assurance reports and understands the impact of the issues raised in these reports.

Source: Victorian Auditor-General's Office.

Remediation of service organisation control weaknesses

While there has been an increase in public sector entities obtaining service assurance reports, there has been limited monitoring undertaken to ensure that the service organisations are remediating the controls weaknesses identified in a timely manner. As a result, commencing in 2014–15, we are summarising the relevant audit findings in our management letters and will regularly check that activities to address these control weaknesses are monitored by management.

We identified one instance where a public sector entity was able to hold their service organisation to account and influence it to strengthen certain aspects of its IT control environment—access controls to IT systems and financial data by the vendor's staff have been strengthened.

2.2.2 Use of IT systems that are end-of-life

Our observations

It is essential that public sector entities ensure that their IT systems have appropriate vendor support. ‘End-of-life’ generally refers to when a vendor intends to stop marketing or supporting a piece of IT software or an application. For example, Microsoft Windows XP's extended support ended in April 2014. Vendors typically indicate to their customers in advance when such support arrangements will cease, to enable a smooth transition to current software prior to a programs end-of-life.

Since 2011–12, as part of our audits, VAGO has reported to in-scope entities which of their financial systems are either approaching end-of-life or past their end-of-life. We inform the entities of the risks posed by continuing to utilise such applications, including new security weaknesses not being fixed by the vendor. Due to the length of time required to implement large scale IT systems, VAGO's approach has always been to flag such issues early and to encourage awareness and proactive remediation activities.

Of particular concern, in 2014–15, was the limited progress by entities in upgrading end-of-life systems. We found audit findings relating to IT systems approaching end-of-life or past their end-of-life at 53 per cent of our in-scope entities. The majority of these 34 end-of-life audit findings were related to key financial systems, including Oracle Financials. Findings also related to software on users' desktops computers, such as Windows XP.

Insights and implications

Our analysis of these findings identified the following issues.

Whole-of-Victorian-Government enterprise resource planning re-implementation

Following the November 2014 change of government and subsequent January 2015 machinery-of-government changes, a project to review and implement a whole-of-Victorian-Government enterprise resource planning (ERP) system was suspended. As a result, the financial systems for many in-scope entities are either approaching end-of-life or are past their end-of-life. Given the current situation and the time required to implement an ERP system, this issue is expected to remain unresolved for some time.

Cost of maintaining obsolete software

As an interim measure, a number of public sector entities have entered into customised contractual arrangements with vendors for the support of obsolete IT software. These arrangements typically come at a significant cost and some vendors increase the cost over time as the use of the program declines globally. As an example, a one-year custom support arrangement for Microsoft Windows XP was renewed by a department in April 2015 at a cost of $2.37 million.

2.2.3 IT security controls need improvement

Our observations

Our IT security findings relate to the following IT general controls categories:

- user access management
- authentication controls
- audit logging and monitoring of IT environment
- patch management
- other IT general controls, including malware protection, penetration testing, physical and environment controls, security and architecture and end-of-life.

IT security issues account for 68 per cent of our 2014–15 audit findings. This is a nominal increase of 1 per cent on the prior year and once again highlights the need for a continued focus on remediating IT security weaknesses.

Most notably, in 2014–15 we have reported an extreme-risk rated audit finding relating to authentication and password controls at one entity. This is detailed in Figure 2D.

Insights and implications

User access management

As described in Part 3 of this report, user access management is the most prevalent issue, accounting for nearly 30 per cent of all our findings. Nearly all in-scope entities have user access management audit findings, which is consistent with the findings of our ICT Controls Report 2013–14.

Public sector entities need to continuously improve the process of managing system access. There are three root cause of user access management control weaknesses:

- **Poor understanding of access provided**—it is common for VAGO to find user accounts for terminated staff not being disabled or removed. While this can be categorised as an oversight, it is ultimately due to a poor understanding or poor documentation of the access provided to the user, or is due to poor process design. 'Single sign-on' systems can help reduce such issues, and are in place at many in-scope entities, but our findings indicate that this does not solve the problem. A process of systematically recording account ownership and all the system accessible to each staff member is key to ensuring that they are subsequently removed when no longer required.
- **The 'human factor' and manual intervention**—human oversights are likely the reason why access remained on systems after a staff member resigns or no longer requires that access. Such oversights are often related to appropriate parties not being notified when a user changes roles. While it is not possible to completely eliminate the 'human factor', how user access is managed can be heavily influenced by well-defined policies, procedures and processes, by an organisation's culture and tone from the top, and by monitoring controls.
- **Inadequate periodic reviews**—the intent of periodic reviews is to validate user access to systems on an ongoing basis and ensure that this is aligned with business needs. Where not aligned, the access should be modified accordingly. This often works as an independent control in combination with existing process controls. More often than not, periodic reviews are conducted by management but are not sufficiently effective to eliminate instances of excessive access provided. In some instances, periodic reviews only focused on certain elements of the IT infrastructure, resulting in control limitations.

Victorian Government IT security standards

In November 2013, a number of IT security standards were published to take effect from 1 January 2014. Some of these standards relate to identity and access management (IDAM), providing specific guidance on password controls and bringing the overall Victorian IT control framework into alignment with better practices and applicable Commonwealth standards such as the *Australian Government Information Security Manual*.

While compliance with the *Victorian Government's Identity and Access Management (IDAM) Standard 03 – Strength of Authentication Mechanism v1.0* is mandatory for all departments and 11 audited agencies, our IT audits found a large number of issues related to password controls. Typical audit findings include:

- entities which have not updated their password policies and procedures to reflect the standard's requirements
- password settings implemented on in-scope systems did not comply with the standards.

This is disappointing given that the Victorian Government IT security standards have been in effect for the full financial year, and agencies have had time to develop an implementation plan.

Through our interaction with management, we believe that there is a general lack of awareness of the Victorian Government IT security standards. Going forward and recognising that there may be changes introduced by the Commissioner for Privacy and Data Protection, VAGO intends to further assess entities compliance with the Victorian Government IT security standards.

At one of our audited entities, we found an extreme risk surrounding authentication controls, which is not consistent with Victorian Government IT security standards. This example is detailed in Figure 2D.

Figure 2D
Case study: Extreme risk surrounding authentication controls

A public sector entity was found to have password management policies and configurations that are not consistent with Victorian Government IT security standards. Ordinarily, such an audit finding would be rated as high risk, however, this case was rated as an extreme risk based on the sensitive and confidential nature of the data that is stored by the entity.

Our review identified that the entity's password management policies are either silent on a number of key password requirements, or the requirements were not strong enough. Audit testing identified numerous instances where the system password configurations were neither aligned with the Victorian Government IT security standards, nor aligned with approved internal standards.

We have highlighted these audit findings for the attention of IT senior management and the audit committee, with responses from both parties being positive and encouraging. Given its risk rating, management expedited the implementation of our audit recommendations.

Source: Victorian Auditor-General's Office.

Recommendations

1. That the Commissioner for Privacy and Data Protection provides education and training to relevant entities on the requirements of the Victorian Protective Data Security Standards—once issued.
2. That the Department of Premier & Cabinet monitors and reports the status of information technology obsolescence risks at departments and public sector agencies.

That public sector entities' governing bodies and management:

3. enhance management's understanding of their *Financial Management Act 1994* and Standing Directions obligations, and ensure:
   - assurance reports received for outsourced information technology environments are reliable and fit-for-purpose
   - exceptions raised in assurance reports are assessed for the impact they may have on the entity's control environment.

Recommendations – *continued*

That public sector entities' governing bodies and management:

4. manage the continuity of vendor support for systems approaching end-of-life, including its upgrade or migration to fully supported solutions. Where possible, entitles should work collaboratively to address information technology obsolescence risk across the public sector
5. implement appropriate governance and monitoring mechanisms to ensure:
   - information technology audit findings are addressed by management
   - sustainable process improvements, to prevent future recurrence
6. align information technology control frameworks to relevant Victorian Government information technology security standards.

3 Results of IT audits

At a glance

Background

For each of the 45 entities selected for this report, we prepared management letters highlighting any control weaknesses identified by our information technology (IT) audits. For this report, these management letters were analysed to identify the overarching themes and key messages that may have a broader impact.

Conclusion

Our financial audits continue to identify a large number of IT control deficiencies. Most of the IT audit findings identified are rated medium and high risk. The number of high-risk findings has increased from 69 in 2013–14, to 134 in 2014–15. One audit finding was rated an extreme risk, to reflect its importance to the entities control environment.

Despite the identified IT controls deficiencies, entities' control environments were reliable for financial reporting purposes, as satisfactory mitigations were in place, such as compensating management controls or alternative audit procedures.

Findings

- User access management and authentication controls continue to be frequently reported high-risk findings, highlighting the need for improvement in this area.
- Other prominent high-risk findings related to:
  - patch management
  - backup management, business continuity and IT disaster recovery planning
  - other IT general controls, namely, third-party assurance and high-risk systems either past, or approaching their end-of-life.

Recommendations

- That public sector entities' governing bodies and management ensure that, where relevant, shared service providers implement disaster recovery frameworks which prioritise IT systems recovery in the event of a disaster impacting a number of departments and agencies.
- That the Department of Premier & Cabinet monitors and reports the status of the implementation of disaster recovery frameworks and plans by shared services boards.

3.1 Introduction

This Part provides a high-level analysis of our 2014–15 information technology (IT) general controls audits.

The audit findings were analysed according to:

- **ratings and categorisation**—extreme, high, medium and low, as explained in Part 3.3, with further detail in Appendix A
- **IT general controls category**—for example, user access management and authentication controls
- **sector**—the sector analysis within this report will largely focus on four sectors; environment and water, departments and central agencies, health and human services and justice.

These audit findings are also used for our maturity assessment of the IT controls environment at the in-scope entities, as reported in Section 3.6.

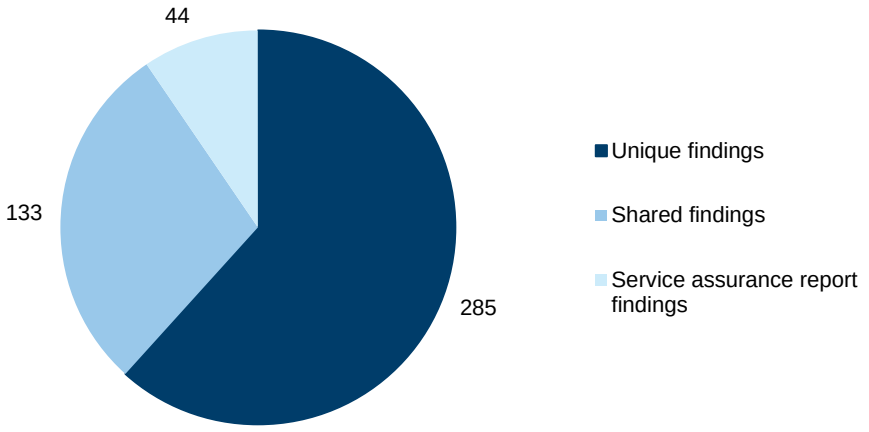
3.2 2014–15 IT audit results

For the 45 selected entities for the 2014–15 financial year, 462 new and previously identified IT audit findings were reported. This represents an increase of 27 per cent compared with the prior year, however there was a 15 per cent increase of in-scope entities.

As shown in Figure 3A, of these audit findings:

- 133 were shared findings as a result of IT environments being shared across entities
- 44 were identified from outsourced IT service assurance reports, which are discussed as a theme in Part 2 of this report.

Figure 3A
Total new and prior-year audit findings not addressed



Source: Victorian Auditor-General's Office.

3.3 IT audit findings ratings and categorisation

3.3.1 Introduction

All VAGO IT audit findings are assigned a risk rating. The rating reflects our assessment of both the likelihood and consequence of each identified issue and assists management to prioritise remedial action.

Audit findings for 2014–15 are rated extreme, high, medium and low risk, further details are found in Appendix A. Through the reporting process, ratings for audit finding are subject to review by management of the in-scope entities.

For the purposes of the *Financial Systems Controls Report 2014–15*, audit findings are also categorised into the following categories for analysis:

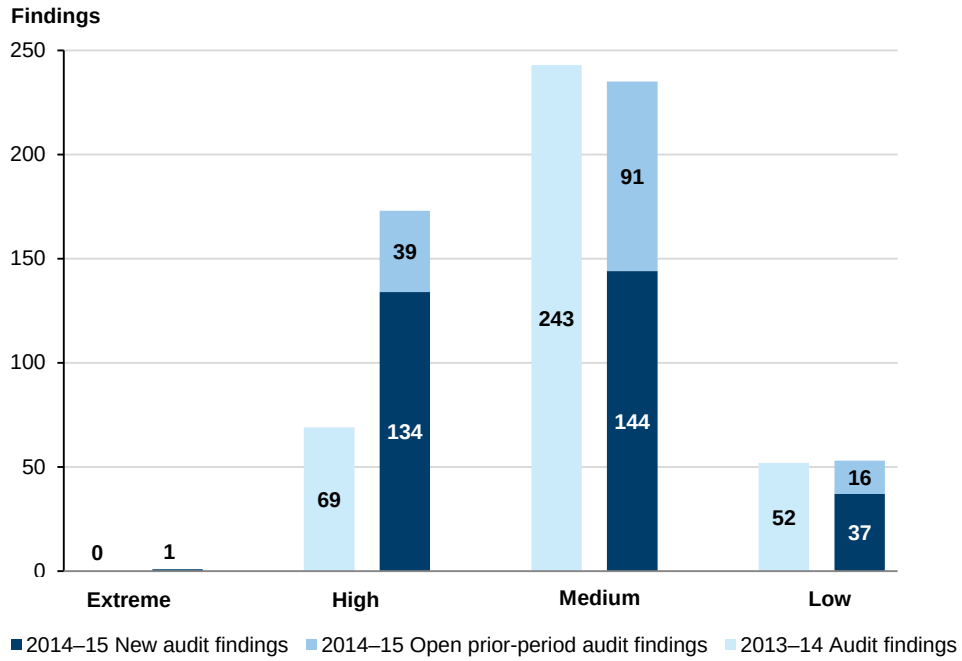
- user access management
- authentication controls
- audit logging and monitoring of the IT environment
- IT change management
- patch management
- backup management, business continuity and IT disaster recovery planning
- other IT general controls.

Other IT general controls are a collection of audit findings that do not necessarily correspond with the above groups. Controls in this category are detailed in Section 3.4.7 of this report.

Analysis of audit findings by risk rating

Figure 3B show an analysis of findings by risk rating and whether the findings were new or prior-year findings.

Figure 3B
Findings by risk rating—new and prior year audit findings not addressed



Source: Victorian Auditor-General's Office.

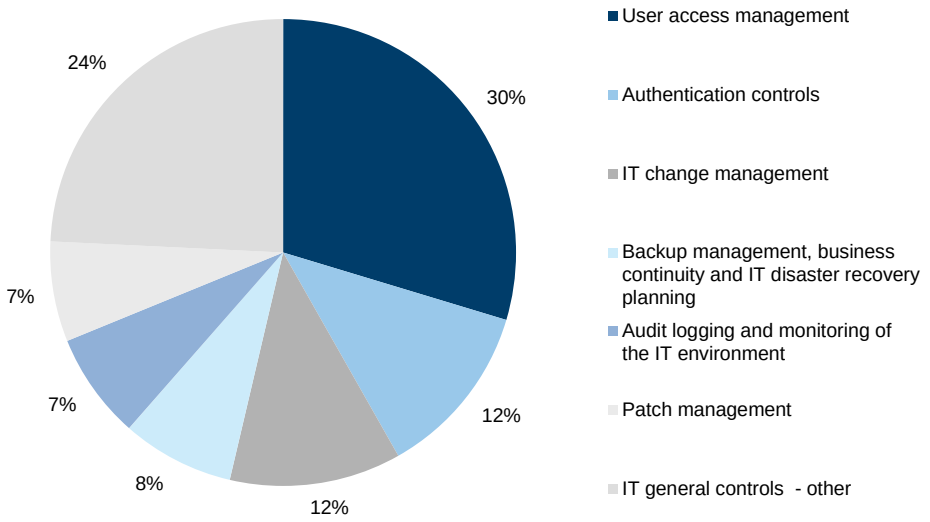
As Figure 3B shows:

- consistent with prior years, most audit findings were rated as medium risk.
- one extreme-risk rated audit finding was identified during 2014–15, in contrast to 2013–14 when no extreme-risk rated audit findings were raised
- despite the 27 per cent increase in the total number of audit findings as compared with prior years, the total number of medium- and low-risk findings have remained relatively stable with the biggest increase being high-risk audit findings, from 69 in 2013–14 to 134 in 2014–15. This is due to an increased number of audit findings in areas such as user access management, IT change management and systems approaching their end-of-life, which are elaborated on, later in this Part.

Analysis of audit findings by category

Figure 3C highlights the percentage of IT audit findings in each IT general controls category.

Figure 3C
Findings by IT general controls category



Source: Victorian Auditor-General's Office.

In 2014–15, an analysis of audit findings by category noted that:

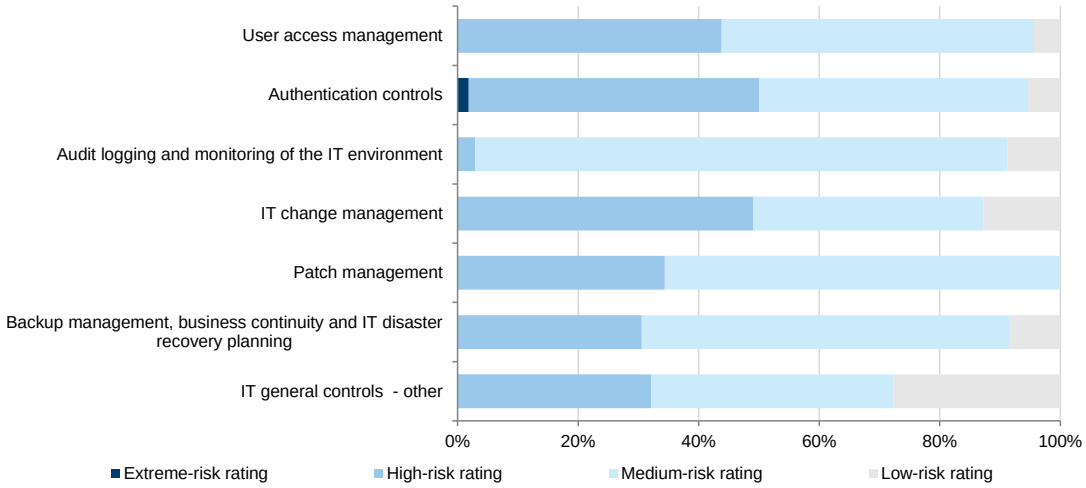
- consistent with the prior year, our findings mostly related to the user access management and authentication controls categories
- while findings related to IT change management only increased 4 per cent against all IT audit findings, this category registered a marked increase from 28 findings in 2013–14 to 54 in 2014–15
- there is a marginal increase in audit findings categorised under the 'other' category (refer to Section 3.4.7), which is attributable to slight variations in VAGO's overall audit approach:
  - there was an increased coverage of our areas of focus; identity and access management, and software licensing, as discussed in Part 4 of this report
  - there was a reduced focus on controls related to penetration testing, physical and environmental controls.

The user access management, authentication controls and other categories account for 66 per cent of all reported findings in 2014–15.

Analysis of audit findings by category and risk rating

Figure 3D shows the distribution of risk ratings within each category.

Figure 3D
Audit findings by risk ratings



Source: Victorian Auditor-General's Office.

In 2014–15:

- an extreme-risk rated audit finding was identified in the authentication controls category, but no other categories had an extreme-risk audit finding
- the categories of authentication controls, user access management, IT change management and other are more likely to have high-risk audit findings. Findings relating to these areas include:
  - password controls do not comply with leading practices or government IT standards
  - excessive numbers of users having administrator access to systems
  - financial systems in use that are either past or approaching their end-of-life and may not be supported by the vendor.

3.3.2 Remediation of prior-period IT audit findings

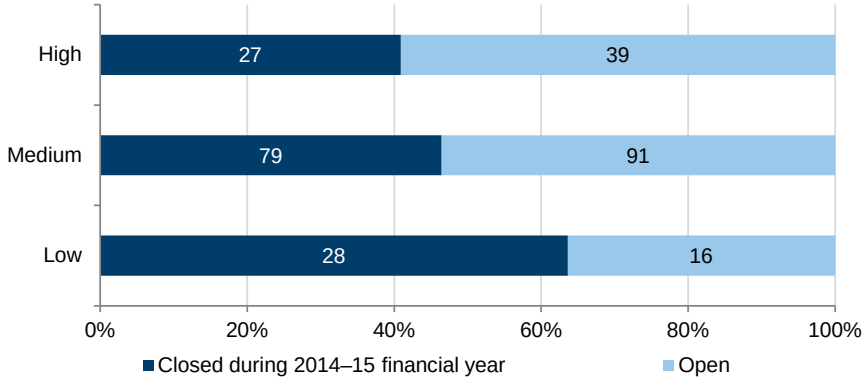
For each of our audit findings the entity's management is required to commit to a date to implement remedial actions. As part of our IT general controls audit, VAGO tracks the audit findings raised and the status of management's remediation.

In 2013–14 VAGO raised 280 IT audit findings and 84 were identified from outsourced IT service assurance reports. Of these 364 IT audit findings 218 (59 per cent) are now considered 'closed'.

Prior to 2014–15, audit findings from assurance reports were not re-reported in VAGO's management letters. These findings were, however, included in the *Information and Communications Technology Controls Report 2013–14* (ICT Controls Report 2013–14). As VAGO has now started to report relevant weaknesses arising from assurance reports, all prior-period findings related to assurance reports have been closed and where relevant, new findings raised.

Figure 3E shows the remediation status of the 280 findings raised by VAGO in 2013–14. Forty-eight per cent of prior-period findings have been remediated, this is consistent with 41 per cent of the high-risk findings having been remediated.

Figure 3E
Prior year audit findings closed during the financial year

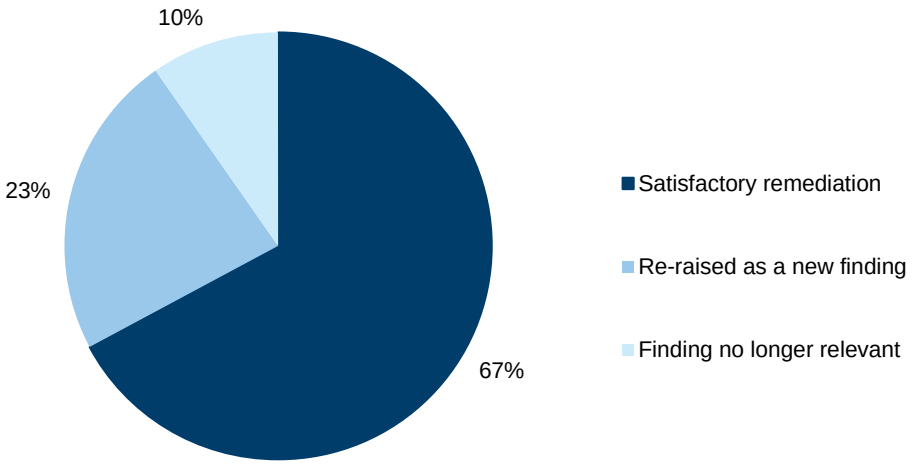


Source: Victorian Auditor-General's Office.

As shown in Figure 3F, findings have been closed for three reasons:

- **Satisfactory remediation**—management has acted on the recommendation and VAGO had not noted similar findings in 2014–15. These closed findings account for 67 per cent of the audit findings closed.
- **Re-raised as a new finding**—VAGO identified a similar finding in 2014–15, which demonstrates that management have not sufficiently remediated the problem. The practice of closing an audit finding and re-raising a new finding enables reporting to be streamlined by not having multiple audit findings relating to the same or similar control weakness. These findings account for 23 per cent of the audit findings closed.
- **Finding no longer relevant**—as a result of changes in an entity's organisation structure or IT environment, prior year audit findings may no longer be relevant or require any further remediation. For example, an IT system may have been decommissioned during the financial year and therefore all findings related to this system are no longer relevant. These findings account for 10 per cent of the audit findings closed.

Figure 3F
Insights on closed audit findings



Source: Victorian Auditor-General's Office.

In 2014–15, while in-scope entities made some progress in remediating prior year audit findings, the following areas still require improvement:

- **Fixing symptoms rather than implementing process improvements**—by not implementing process improvements, new control weaknesses may be introduced. For example, if a process that covers multiple IT systems is not improved, entities may only remediate the systems in-scope for our audit, rather than all IT systems.
- **Ineffective governance**—in-scope entities with strong governance structures are more likely to be proactive and successful in addressing the audit findings and preventing future recurrence. Those with poor governance structures are more likely not to remediate control weaknesses in a timely manner and have recurring audit findings.

3.4 IT general controls categories

3.4.1 User access management

Introduction

User access management relates to the process of managing access to applications and data, including how access is approved, revoked and periodically reviewed to ensure it is aligned with staff roles and responsibilities. User access management's primary objective is to maintain the confidentiality and integrity of IT systems and data.

This category also involves a review of the appropriateness of 'super users', who have wide-ranging authorisation within applications and systems, including the ability to create other users.

Weaknesses in user access management controls may result in inappropriate and excessive system and data access, which could affect the completeness and accuracy of transactions.

Audit procedures performed

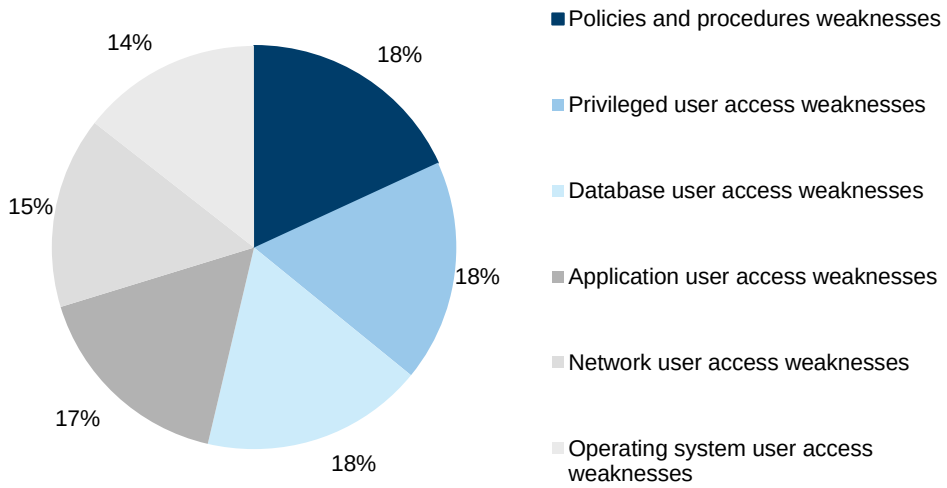
We examined the policies and procedures governing this process, and evaluated the controls implemented by management to ensure access to systems and data is restricted to authorised users who require it for a legitimate business purposes.

Audit findings

A total of 137 user access management findings were reported in 2014–15, representing 30 per cent of total findings and 33 per cent of high-risk audit findings, making this the category with the highest percentage of high-risk findings.

Figure 3G shows an even distribution of audit findings across the IT environment—database, application and operating system—which suggests that improvements are required at all levels.

Figure 3G
User access management audit findings



Source: Victorian Auditor-General's Office.

The 2014–15 results are consistent with last year's results. User account administration findings account for around 80 per cent of the control weaknesses, which is consistent with the prior year. User account administration typically covers matters such as:

- absence of appropriate approval prior to access being granted
- non-removal of user's system access following their termination
- non-review by management to ensure system access rights are aligned to the users role and responsibilities.

3.4.2 Authentication controls

Introduction

Authentication controls assist in determining whether a user attempting to access a system is who they claim to be.

Authentication is commonly performed through the use of passwords, and through the use of two-factor authentication in more tightly managed environments. Two-factor authentication includes something the user knows—i.e. a password—and something the user has—i.e. a security token.

Weaknesses in authentication controls may increase the risk of breaches in the confidentiality, integrity and availability of systems and data.

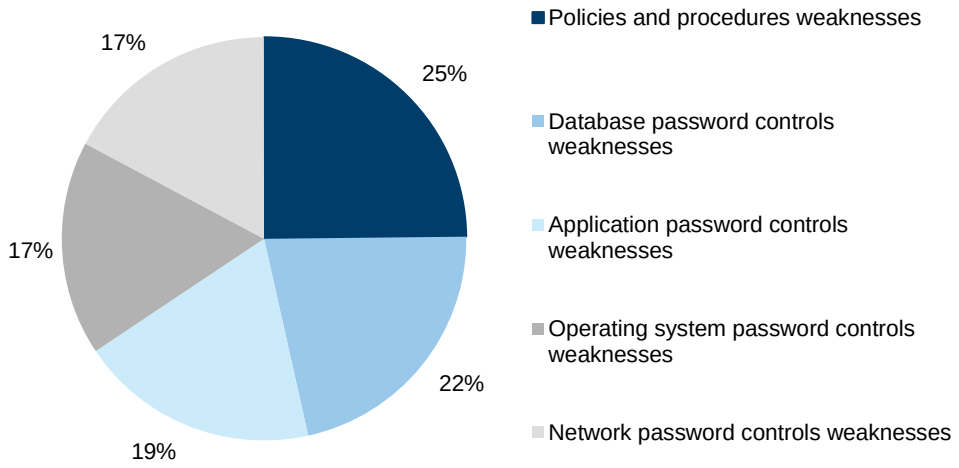
Audit procedures performed

We examined policies and procedures over password controls, and evaluated the password controls implemented by management to restrict access to in-scope IT applications and support infrastructure.

Audit findings

Authentication controls weaknesses accounted for 56 audit findings, or 12 per cent of the total. They accounted for 16 per cent of high-risk audit findings, with one finding rated as an extreme risk. As shown in Figure 3H, authentication controls audit findings are evenly spread across policy and procedure related weaknesses and password control weakness, across all IT components, namely the database, application layer, operating system and network.

Figure 3H
Authentication controls audit findings



Source: Victorian Auditor-General's Office.

In November 2013, a number of IT security standards were published by the former Department of State Development, Business and Innovation (DSDBI) to take effect from 1 January 2014. One of the published standards—the *Victorian Government's Identity and Access Management (IDAM) Standard 03 – Strength of Authentication Mechanism v1.0*—provides specific guidance on password controls and aligns the overall Victorian IT control framework with the applicable Commonwealth standards and better practices, such as the *Australian Government Information Security Manual*. This standard is mandatory for all departments and 11 audited agencies.

Due to this development, in 2014–15 we noted a 20 per cent increase in findings related to entities' password controls that did not comply with these standards.

3.4.3 Audit logging and monitoring of the IT environment

Introduction

Audit logging and monitoring of the IT environment involves the recording and analysing of system and user activities in order to detect and mitigate unusual events within financial systems.

Weaknesses in audit logging and monitoring of the IT environment may lead to an increased risk that inappropriate or unauthorised activities could go undetected by management. Where inappropriate activities have occurred, management may not be able to trace the origins of the event due to incomplete or missing audit trails.

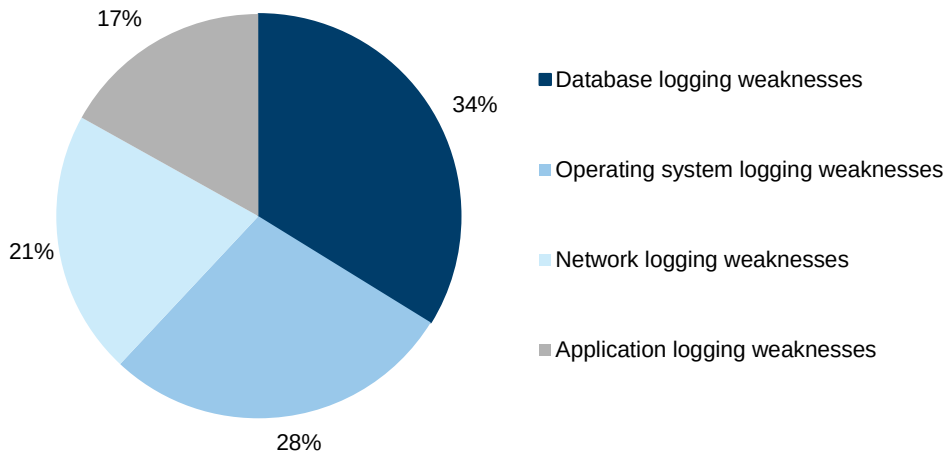
Audit procedures performed

We examined audit logging and monitoring policies and procedures, and evaluated the audit logging and monitoring controls implemented by management.

Audit findings

Audit logging and monitoring of the IT environment control weaknesses accounted for 34 audit findings, or 7 per cent of all findings. There was one high-risk audit finding, with most findings rated medium risk.

Figure 3I
Audit logging and monitoring audit findings



Source: Victorian Auditor-General's Office.

As shown in Figure 3I, most audit logging and monitoring audit findings, accounting for 83 per cent of all audit findings raised, relate to the IT infrastructure level (database, operating system and network), with application logging and monitoring being generally stronger. This result is consistent with prior year.

3.4.4 IT change management

Introduction

The objective of IT change management is to make sure that changes to an IT environment are appropriate and preserve the integrity of underlying programs and data.

Weaknesses in IT change management may lead to unauthorised changes being made to systems and programs. This could impact the integrity of the data of underlying financial systems.

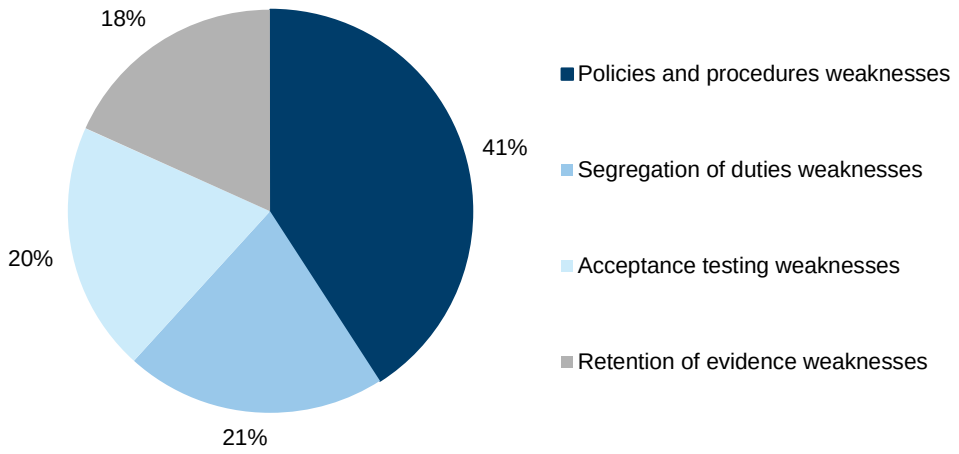
Audit procedures performed

We examined the policies and procedures governing IT change management. Where appropriate, we performed sample testing of changes to in-scope IT applications to validate whether the changes were appropriately authorised, tested and approved.

Audit findings

IT change management control weaknesses accounted for 55 audit findings, or 12 per cent of the total identified findings.

Figure 3J
IT change management audit findings



Source: Victorian Auditor-General's Office.

As shown in Figure 3J a significant percentage (41 per cent) of IT change management findings relate to improvements required to policy and procedures. Change management policy and procedures drive operational processes. The other audit findings relating to change management were fairly evenly distributed among the following control activities:

- **segregation of duties**—change management staff have access to both production and non-production environments, such as development and test environments, increasing the risk that staff may both develop changes and implement them without appropriate oversight
- **acceptance testing**—inadequate levels of testing performed as part of the change process
- **retention of evidence**—insufficient documentation is retained to demonstrate that key controls are being performed.

3.4.5 Patch management

Introduction

A patch is an additional piece of software released by vendors to fix security vulnerabilities or operational issues. Periodic patching aims to reduce the risk of security vulnerabilities in systems and enhance the overall security profile of the IT infrastructure.

Where patches are not applied on a periodic basis, security vulnerabilities remain exposed. This may result in unauthorised access to systems and data, and increases the risk of financial, operational and reputational loss.

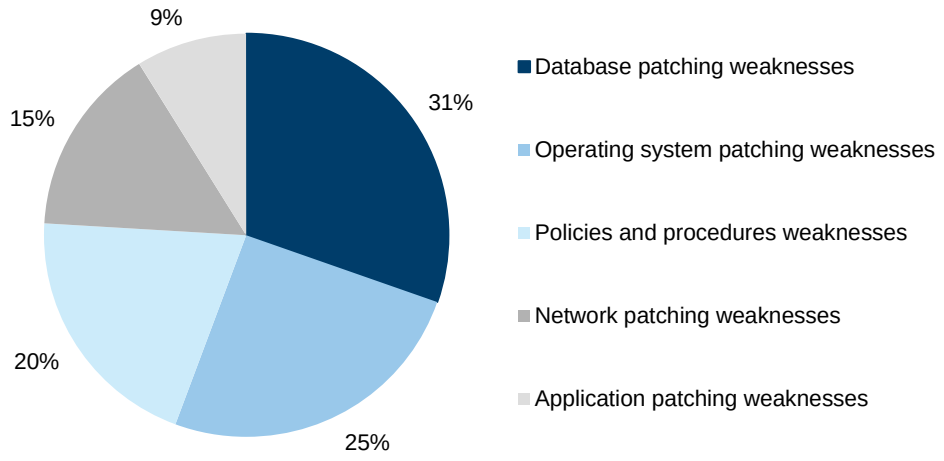
Audit procedures performed

We examined policies and procedures over patch management, and validated that in-scope IT applications have been patched by management in accordance with policies and recommended industry practices.

Audit findings

Patch management control weaknesses accounted for 32 audit findings, or 7 per cent of the total identified findings. These audit findings account for 6 per cent of our high-risk findings. Figure 3K shows most IT change management findings related to database patching, operating system patching and policy and procedures. Collectively, these accounted for 76 per cent of all our patch management findings.

Figure 3K
Patch management audit findings



Source: Victorian Auditor-General's Office.

Patching was highlighted as one of the themes in last year's ICT Controls Report 2013–14, as an area requiring improvement. While we have seen improvements in 2014–15, the number of findings in this area has increased slightly from 26 last year. This increase is due to:

- entities who have done little to improve patch management processes
- new entities or systems subjected to IT audits.

In certain instances, where the process had not improved sufficiently, VAGO had elevated the risk rating to ensure management pays adequate attention to the matter.

3.4.6 Backup management, business continuity and IT disaster recovery planning

Introduction

Backup management, business continuity and IT disaster recovery planning involves the identification of the entity's business continuity requirements and data backup needs.

A business continuity plan details the response strategy of an organisation in order to continue operations and minimise the impact in the event of a disaster. An IT disaster recovery plan is a documented process to assist in the recovery of an organisation's IT infrastructure in the event of a disaster.

Weaknesses in backup management, business continuity and IT disaster recovery planning may impact the ability of an organisation to recover its critical systems and transactions in a complete and timely manner.

Audit procedures performed

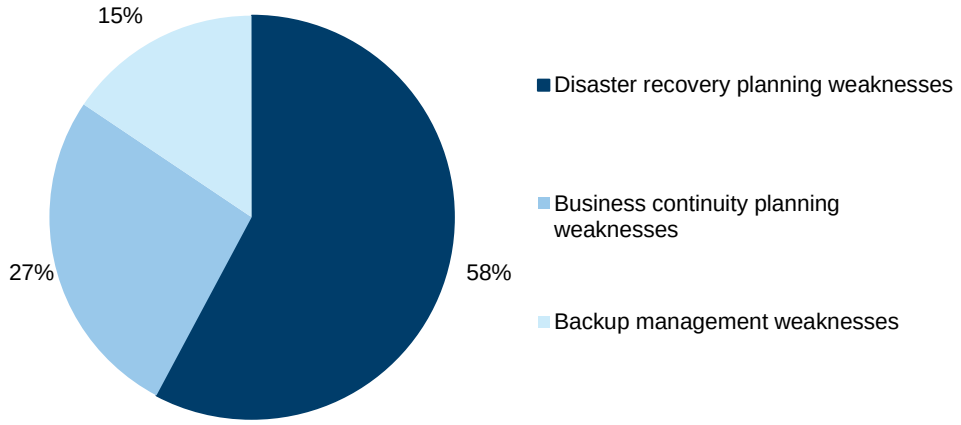
We examined each organisation's policies surrounding data backups and the framework for business continuity and disaster recovery planning. Testing involved:

- examining whether backups are performed as intended, and whether data is periodically tested and recoverable
- examining if business continuity and disaster recovery plans exist, are updated, and are periodically tested by management.

Audit findings

Collectively, backup management, business continuity and IT disaster recovery planning accounted for 36 audit findings, or 7 per cent of the total findings. Weaknesses in this category represent 6 per cent of our high-risk findings.

Figure 3L
Backup management, business continuity and IT disaster recovery audit findings



Source: Victorian Auditor-General's Office.

Figure 3L shows consistent results to the prior year, with the absence or limitations in disaster recovery planning accounting for 58 per cent of our findings, compared to 57 per cent the prior year. Fewer findings are raised in relation to backup management indicating this is better managed by entities, and this can act as a compensating control.

Disaster recovery planning was highlighted as a theme in last year's ICT Controls Report 2013–14 and while not reported as a key theme in this report, it still remains a significant concern. 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. This is of particular concern where a number of department and agencies are dependent on the one IT service provider, as there may be resource challenges and differing views on priorities if such an event were to occur.

Specifically, the following had been noted:

- The service provider does not have sufficient IT disaster recovery capability to respond to a significant event.
- Departments and agencies are not informing themselves adequately about the service provider’s IT disaster recovery capability.
- Because it is unassessed and unmanaged, the potential risk of IT failure after a significant event can be significant and unacceptable.
- Although the service provider had advised the departments and agencies in its annual attestations that it does not have an IT disaster recovery plan to address significant failures, there had been no action by the service provider to address the risk.

An inability by the departments and agencies, and their IT service providers, to react and respond appropriately could result in an interruption to the delivery of services to the community and reputational damage to the state and the entities involved.

3.4.7 Other IT general controls

All the remaining IT audit findings have been included in the category 'other'. These findings include:

- **IT systems at their end-of-life**—relates to cases where the system vendor has, or is intending to stop or limit support for its product in the near future.
- **Controls at outsourced IT environments**—relates to the assurance that third-party service providers are designing and operating appropriate controls over outsourced financial systems.
- **Software licensing**—relates to controls implemented to manage the purchasing and deployment of software and ongoing compliance throughout its use.
- **Governance**—relates to entity-level controls including overarching frameworks, policies and standards.
- **Physical and environmental controls**—relates to physical access to the IT infrastructure and environment controls, such as appropriate temperature and humidity controls, and continuity of power supply.
- **Malware protection**—relates to protection of network and computer systems from malicious software designed to cause disruption or damage to systems.
- **Identity and access management**—relates to how individuals are provided with an appropriate level of access to data and information, and aims to reduce inappropriate access.
- **Security and architecture**—relates to vulnerabilities or limitations in the organisation's network security configuration or management framework.
- **Penetration testing**—relates to the process and outcomes of a technical evaluation of the internal and external vulnerabilities of IT systems.

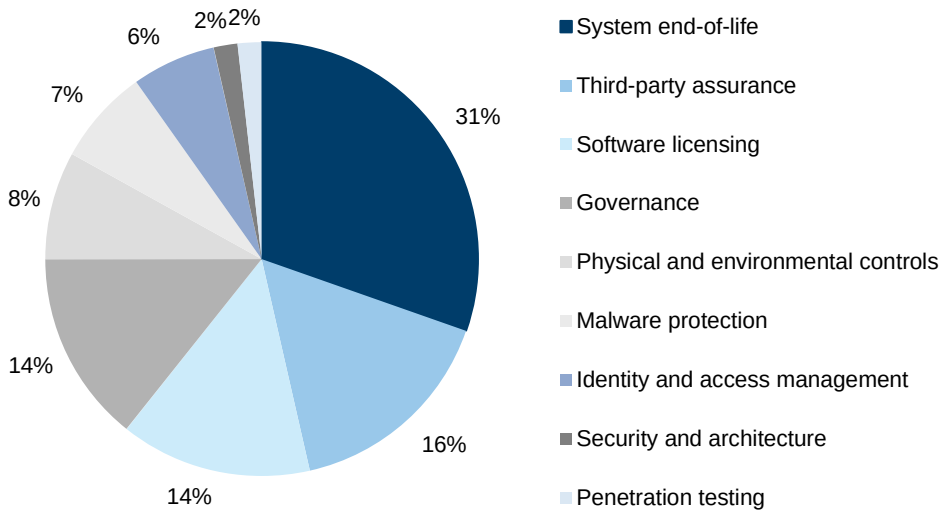
In 2014–15, changes in VAGO's IT audit methodology resulted in the areas of physical and environmental controls, security and architecture, and penetration testing being a lesser focus.

Audit findings

Collectively, 'other' control weaknesses accounted for 112 audit findings, or 24 per cent of the total number of findings, and representing 25 per cent of high-risk findings. Unlike other categories where the number of audit findings have either remained largely similar or have increased, the audit findings within this category have decreased from the prior year. Much of this is attributable to a slight variation in VAGO's IT audit methodology for 2014–15.

Notably, audit findings relating to controls at outsourced IT environments and system end-of-life continue to dominate our attention and represent two of our three key themes for 2014–15. Eighty-nine per cent of the high-risk findings in this category relate to these two audit findings. Refer to Figure 3M for 'other' IT general controls audit findings.

Figure 3M
'Other' IT general controls audit findings



Source: Victorian Auditor-General's Office.

3.5 Audit findings by top four sectors

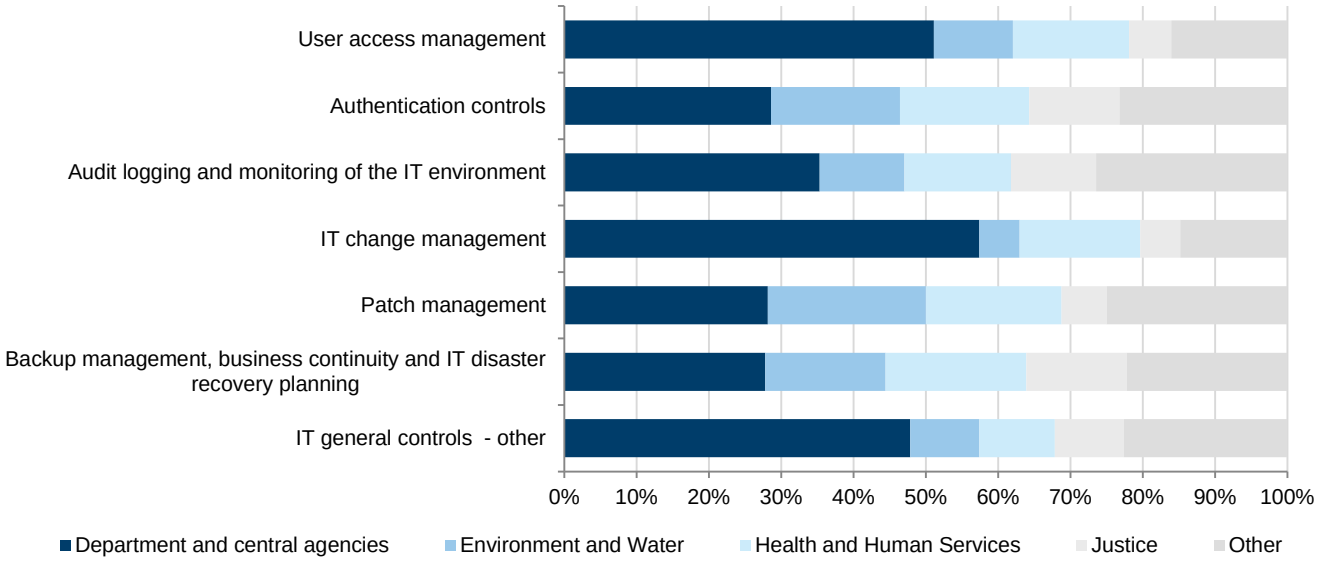
There are four sectors which represent about 74 per cent of our in-scope entities:

- **Departments and central agencies**—large portfolio departments and entities which administer centralised government functions. In-scope financial systems used by departments and central agencies typically include financial reporting and general ledger systems, with revenue and payroll systems also fairly common. The sharing of IT systems within this sector is common and most entities using the IT services of CenITex.
- **Environment and water**—comprises metro, regional and rural water corporations. Key financial systems in-scope for entities in this sector relate to revenue and billings processes. From an IT perspective, there are relatively low levels of shared service arrangements, compared to other sectors.
- **Health and human services**—includes hospitals and entities related to the provision of healthcare services. While most of these entities are located within metropolitan Melbourne, a couple of entities within regional Victoria have also been included in this report. Financial systems in-scope for this sector are typically financial reporting and general ledger systems. Some of the in-scope entities within this sector participate in shared service arrangements and receive service assurance reports over the outsourced IT control environment.

- **Justice**—comprises emergency services and entities involved in law enforcement. In-scope financial systems within this sector mostly relate to the financial reporting and general ledger systems. A number of entities within this sector share key financial systems and there are also a number of outsourced IT arrangements to both CenITex and the private sector.

Figure 3N shows the percentages of audit findings attributable to the top four sectors. Departments and central agencies account for only 17 per cent of our total in-scope entities, and are over-represented in the number of audit findings.

Figure 3N
Audit findings for top four in-scope sectors



Source: Victorian Auditor-General's Office.

Figure 3O summarises our findings for the top four sectors by IT general controls categories:

- While in-scope entities in the top four sectors had relatively high numbers of reported IT audit findings, some sectors performed better than others. The environment and water sector has the most in-scope entities, but has a lower number of audit findings and conversely, the justice sector has fewer in-scope entities but a larger number of audit findings reported.
- A high number of findings are reported for departments and central agencies. Audit findings in this sector are more prevalent at the IT infrastructure levels—network, operating systems and database layers—as opposed to the application layer. This reflects the fact that their IT infrastructure is mainly managed by a shared service provider, while their applications are managed by internally.
- While user access management weaknesses are fairly pervasive across our top four sectors, they are most prevalent in departments and central agencies.

- The health and human services sector requires improvement in a number of user access management areas, with application user access management being a key weakness.
- The environment and water sector, despite being the sector with the most in-scope entities, fared relatively well when compared to other sectors, especially in relation to application and operating system user access management.
- A relatively high number of audit findings was raised for in-scope entities in the justice sector. The justice sector had a lower number of network-related audit findings due to limited coverage of this IT infrastructure layer at our in-scope entities.
- Malware protection, and physical and environmental control audit findings are reported extensively for departments and central agencies as compared with other entities. This is due to our past practice of only auditing larger entities for these aspects of IT general controls.

Figure 3O
Distribution of audit findings across the top four sectors by information technology general controls category

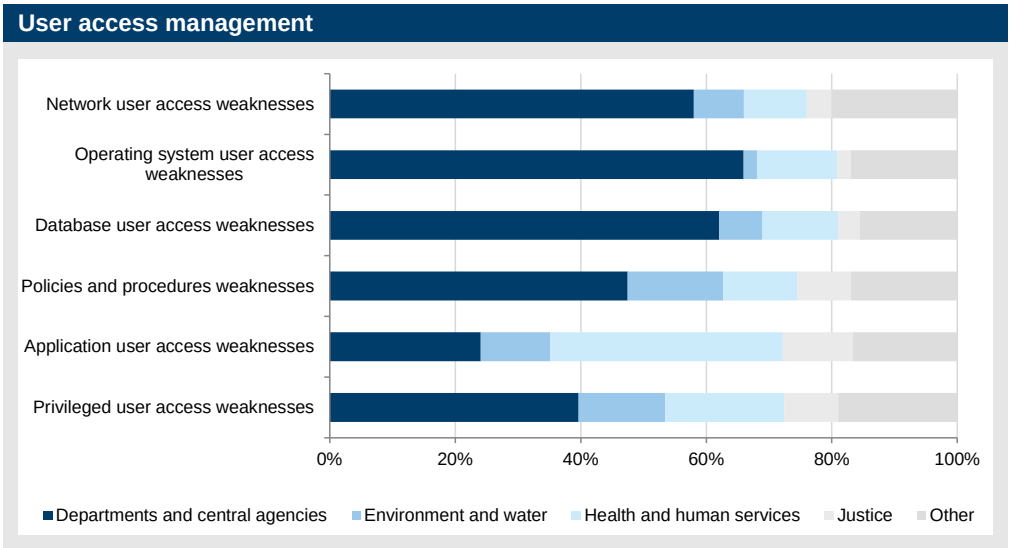


Figure 3O
Distribution of audit findings across the top four sectors by information technology general controls category – *continued*

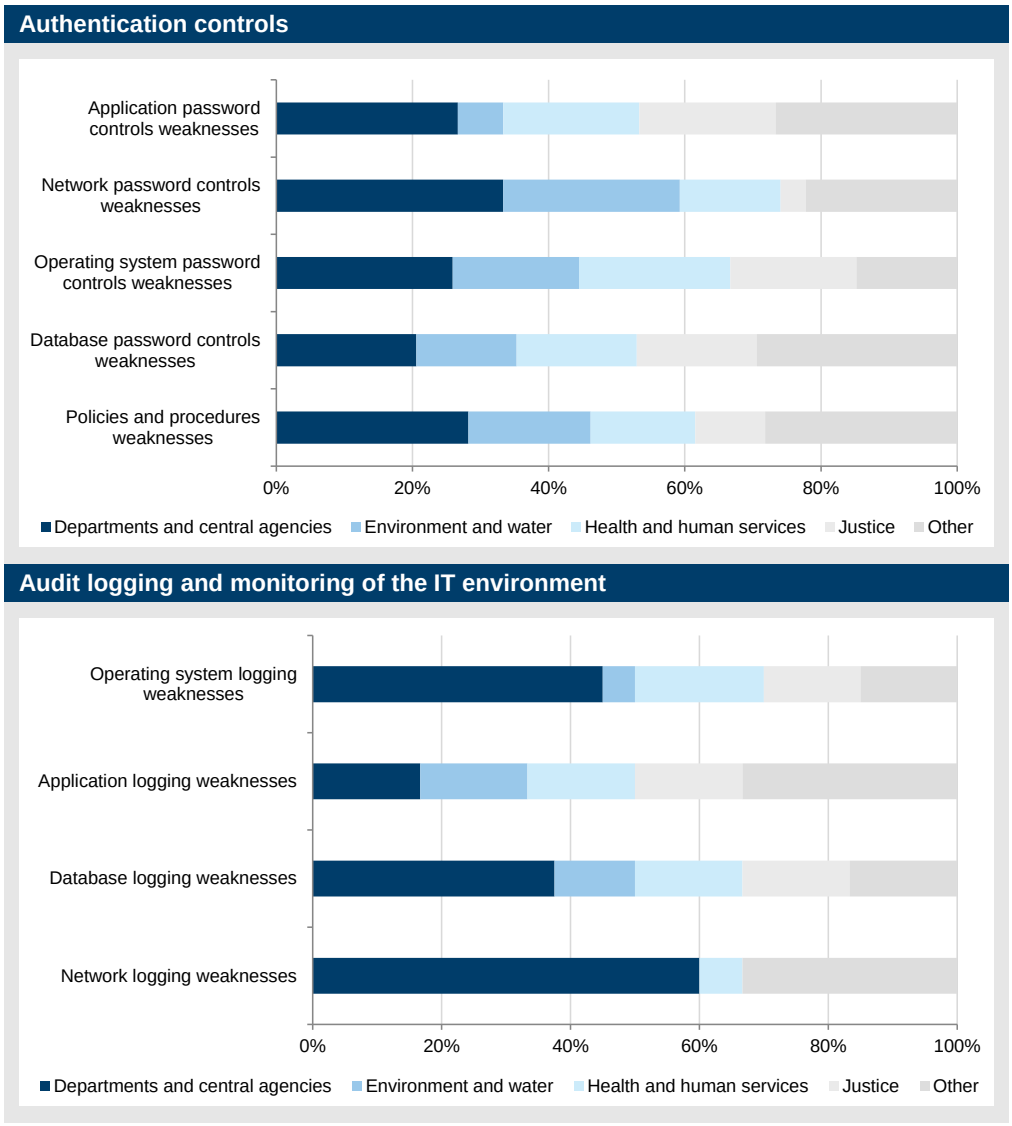


Figure 3O
Distribution of audit findings across the top four sectors by information technology general controls category – *continued*

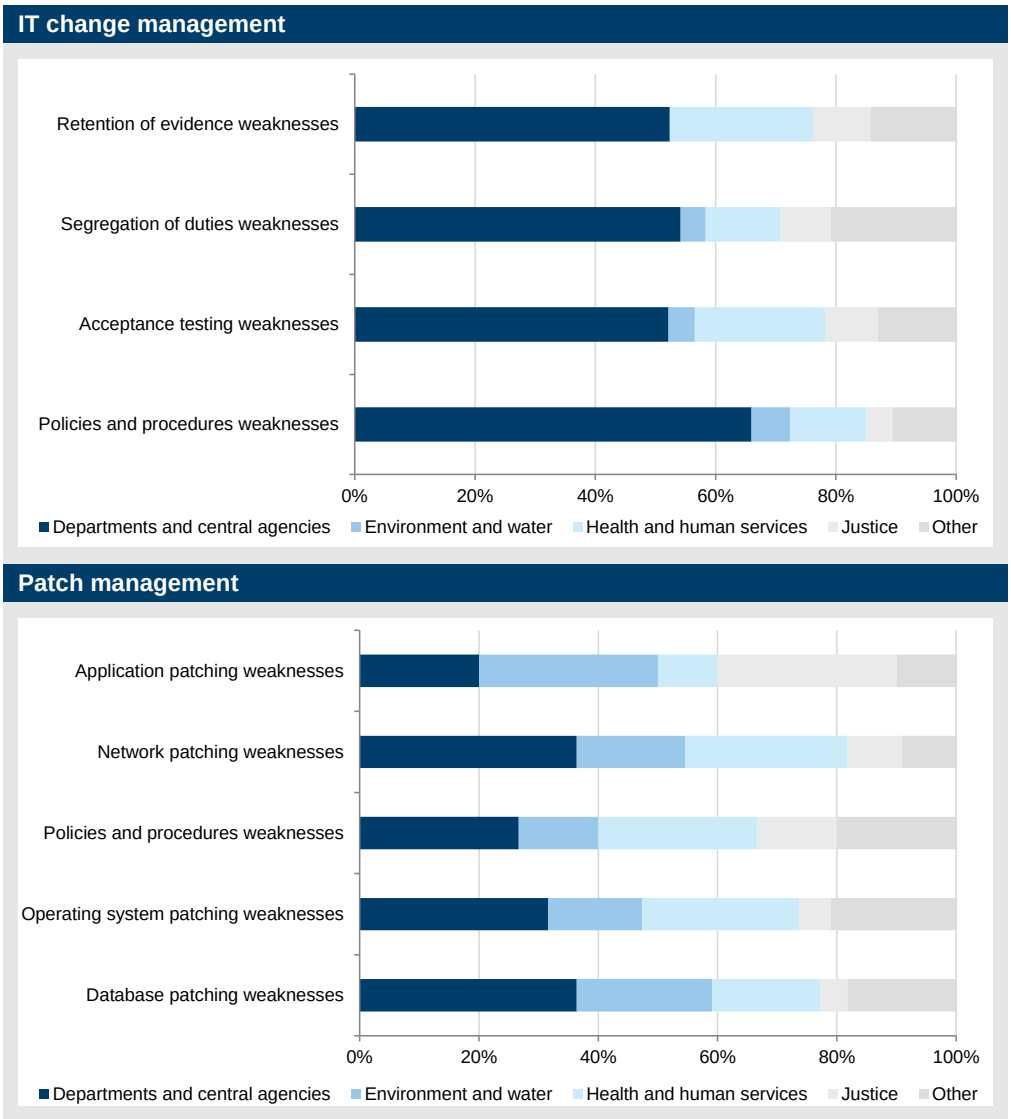
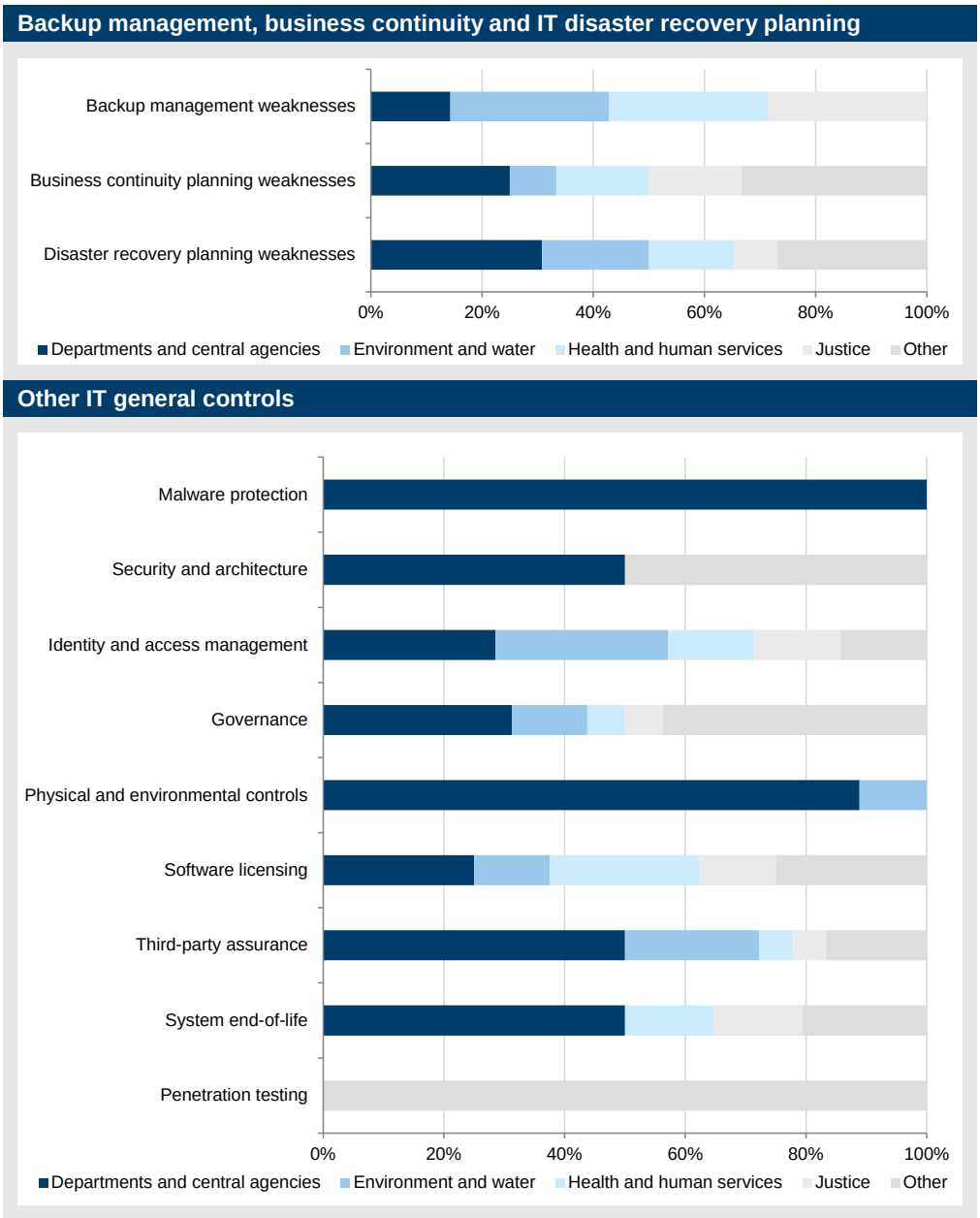


Figure 3O
Distribution of audit findings across the top four sectors by information technology general controls category – *continued*



Source: Victorian Auditor-General's Office.

3.6 Financial systems IT controls maturity assessment

One of the objectives of this report is to use the results of our IT audits to assess the maturity of in-scope entities' controls. Maturity models allow an assessment of how well developed and capable the established IT general controls are, and measure this against an objective baseline.

3.6.1 How did we assess maturity?

Our assessment of entities' IT maturity is based on the audit findings by IT general controls category and by risk rating. Where an entity relies on external agencies or outsourced parties to manage elements of its IT operations, we have incorporated these, so as to present a holistic maturity assessment of the entire environment.

To assess the maturity of IT controls at the audited entities, we adopted the maturity definitions and scores from the Capability Maturity Model Integration (CMMI), tailored to our specific circumstances. The outcomes of the IT control maturity assessment was communicated to senior management of in-scope entities during the 2014–15 audits.

Figure 3P
Maturity level definitions

Maturity score	Description of maturity level
1	**Initial process**—no standardised, sustainable or repeatable process. No strategic review or policies to guide practices. Practices are dependent on individual effort. Policies and procedures, where defined, are ineffective or not being followed.
2	**Repeatable process**—there are some sustainable and repeatable processes, but these may be inconsistent. Key policies to achieve a baseline level of control may exist, but may be ineffective or out-of-date. Policies and procedures may be ill-defined but staff are aware of their role and requirements.
3	**Defined process**—there are defined processes to achieve a baseline level of control and these practices are generally uniformly applied. Key policies exist but good process controls are not pervasive or vigorously enforced.
4	**Managed process**—there are up-to-date and effective strategies, policies and procedures. Best end-to-end practice is in place, is standardised and is enforced. Strong visibility and monitoring. No audit findings were identified though controls tests across the IT systems in-scope, and the IT environment is governed and risk managed.
5	**Optimised process**—proactive and complete risk management and performance. Defined processes are embedded or continually improving the process of managing the systems in-scope. Processes are fully aligned with strategies, policies and procedures. Continuous monitoring drives process improvements. Leading processes are integrated and standardised across the organisation.

Source: Victorian Auditor-General's Office.

When determining the level of desired IT control maturity, VAGO expects entities to strike an appropriate balance between managing entity risks and the level of controls required. A desired maturity score of 5—an optimised process—may not be cost effective. Over time, an entities' process improvements should bring the maturity of controls to the desired level.

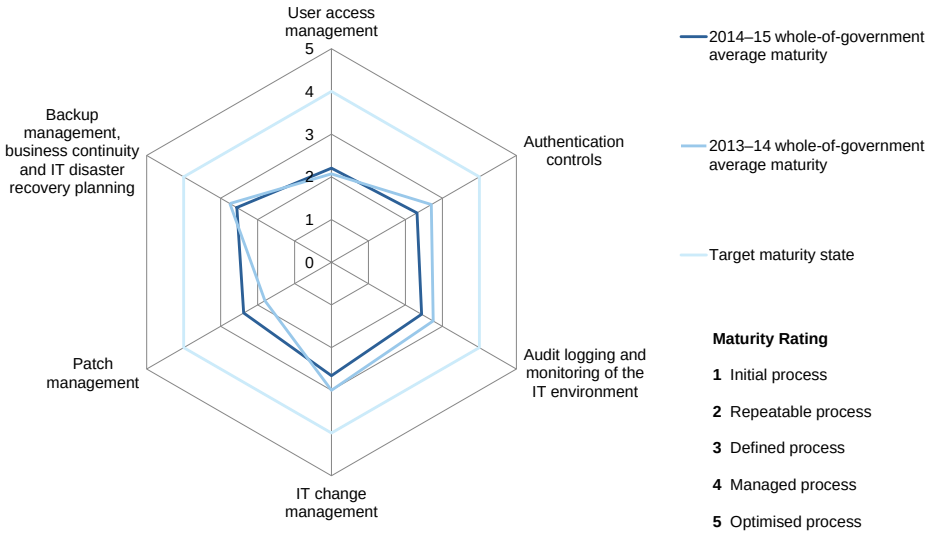
At entities where no audit findings were noted as part of our audit, we would generally score the relevant IT general controls category as having a maturity score of 4. This represents the maturity level we believe public sector entities should be aiming for.

3.6.2 Maturity assessment results

Overall IT controls maturity assessment by category

Figure 3Q shows our maturity assessment scores by IT general controls category for the selected 45 entities. The overall maturity assessment score is derived by averaging the aggregated maturity scores of the in-scope entities, as listed in Appendix B.

Figure 3Q
Overall IT controls maturity assessment for audited entities



Source: Victorian Auditor-General's Office.

The overall IT maturity scores for the 2014–15 show some deterioration from the prior year across most of the IT general controls categories. The category with the most improvement is patch management—the 2014–15 whole-of-government average maturity score is 2.4, compared to 1.8 in the prior year.

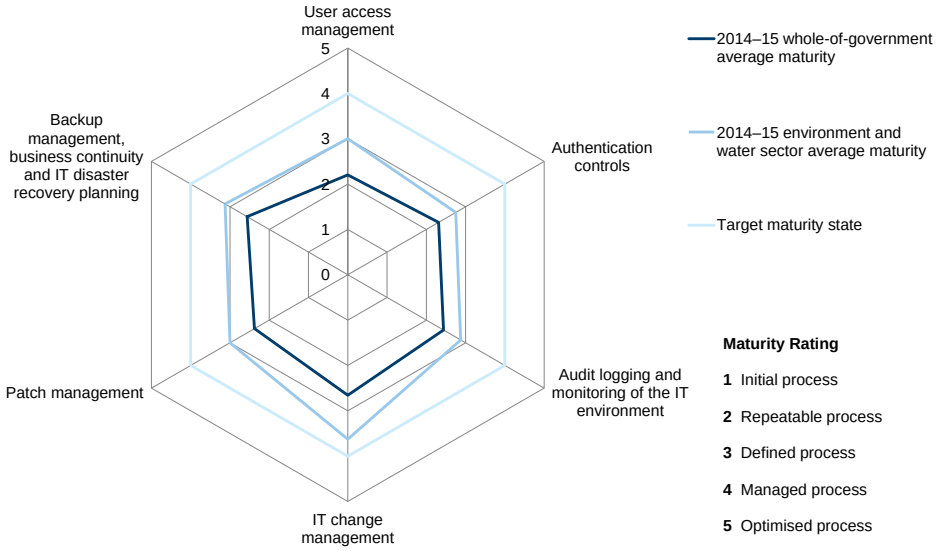
Three categories had low maturity scores, around level 2, meaning controls across IT systems may be inconsistent despite some sustainable and repeatable practices and procedures.

IT controls maturity for top four sectors

Environment and water

Figure 3R shows that environment and water entities are consistently rated as more mature, across all six IT general control categories, than the whole-of-government average.

Figure 3R
Environment and water sector IT controls maturity



Source: Victorian Auditor-General's Office.

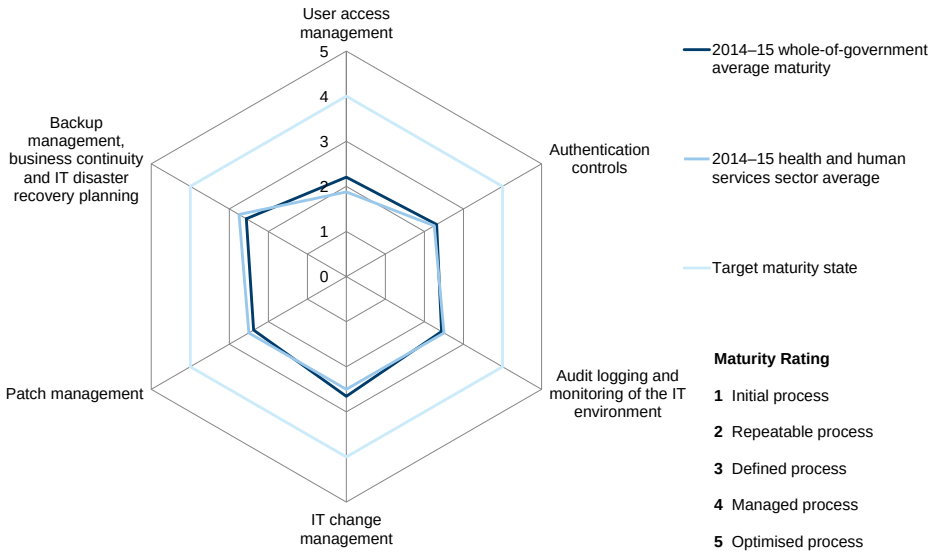
The maturity assessment for this sector identified four categories with a maturity score of 3 or higher, which means that processes are defined to achieve a baseline level of control, however control weaknesses may still exist.

Of the nine in-scope environment and water entities, one entity had higher levels of maturity across all the categories. Another entity was overall less mature than its sector peers due to many control weaknesses being identified at its IT service provider.

Health and human services

As shown in Figure 3S, maturity scores for health and human services in-scope entities are generally lower than the whole-of-government average.

Figure 3S
Health and human services sector IT controls maturity



Source: Victorian Auditor-General's Office.

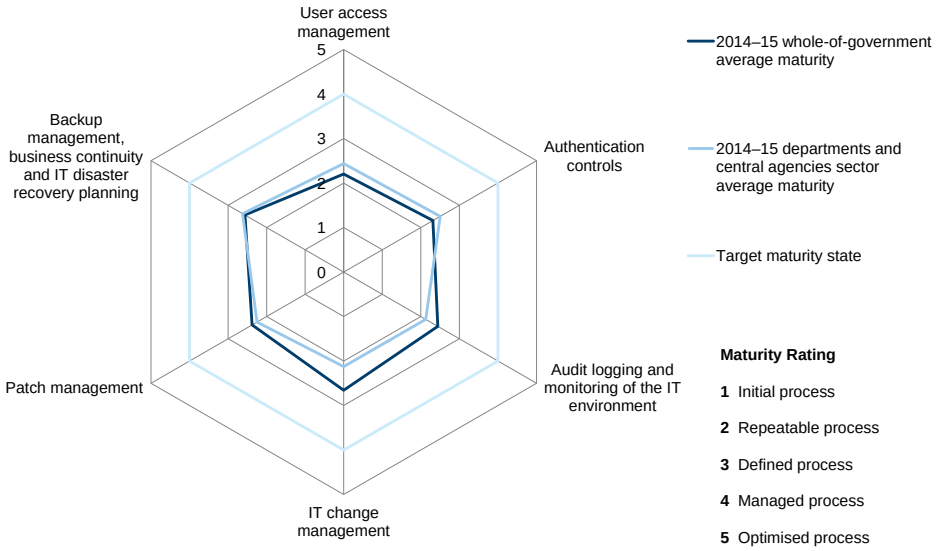
The category requiring most improvement is user access management. At a sector level, our assessment identified this category as being between maturity levels 1 and 2. This means processes surrounding user access management may not be formally documented or guided by policies, and controls could be ad hoc and ineffective.

When compared with the whole-of-government average, business continuity and IT disaster recovery planning processes and controls were more mature in this sector. However, with an average rating of 2.75, improvements are still required.

Departments and central agencies

Figure 3T shows that the maturity scores for in-scope entities in the department and central agencies sector are generally consistent with the whole-of-government average, with change management and audit logging and monitoring of IT environment being more mature than the average across government.

Figure 3T
Departments and central agencies sector IT controls maturity



Source: Victorian Auditor-General's Office.

Due to a significant number of IT audit findings being reported for entities in this sector, the majority of IT general controls categories have a maturity score of 2.

The most mature category in this sector is backup management, business continuity and IT disaster recovery planning. With a sector average maturity score of 2.6, processes in this category are defined to achieve a baseline level of control, however, control weaknesses may still exist.

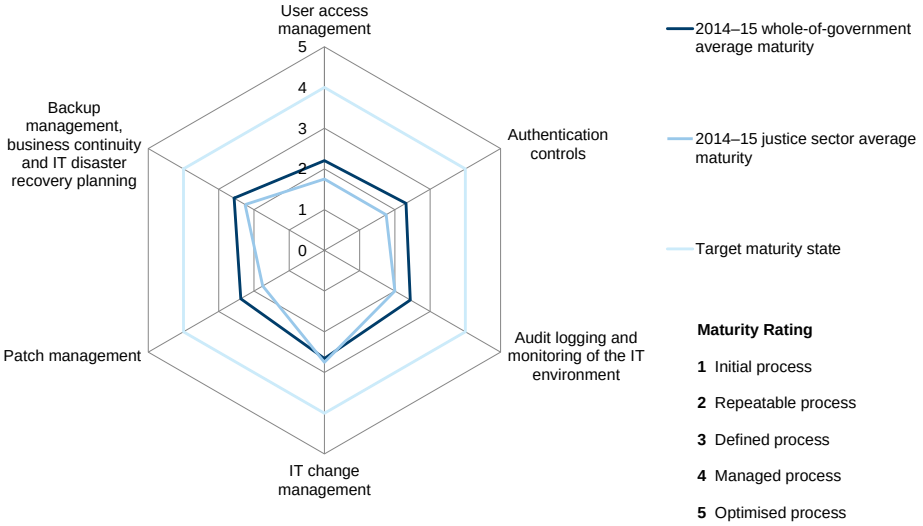
A large number of the audit findings reported in this sector relate to a shared service provider. Because this sector is heavily represented in our audited entities, and will continue to be so in the future, improvements and strengthened controls in the shared service provider's IT environment should lift the maturity level of this sector and the whole-of-government average.

One entity within this sector was rated to be more mature than its sector peers, and the entity does not rely on the shared service provider.

Justice

As shown in Figure 3U, maturity scores for the justice sector are relatively low when compared with the whole-of-government average.

Figure 3U
Justice sector IT controls maturity



Source: Victorian Auditor-General's Office.

Both authentication controls and patch management had scores of 1.8 which means processes within these categories may not be formally documented or guided by policies and procedures, and controls could be ad-hoc and ineffective.

The only category that is rated more mature than the whole-of-government average is IT change management, however with a maturity score of 2.8 this is still far from ideal.

One in-scope entity in the justice sector was rated below the whole-of-government average for every IT general controls category.

3.6.3 Maturity assessment conclusions

During 2014–15, while individual in-scope entities may have noted improvements in their IT control environment, a number of these improvements may not have been sufficiently pronounced to affect our maturity assessment. This is due in part to our assessment being based on the audit findings identified and reported to management. We intend to continue to measure and report on IT controls maturity, as it allows entities to monitor and compare their maturity over time. However, it must be noted that our evaluations are based on the results of our IT audits and therefore subject to our specific scope and analysis.

Recommendations

7. That public sector entities' governing bodies and management 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.
8. That the Department of Premier & Cabinet monitors and reports the status of the implementation of disaster recovery frameworks and plans by shared services boards. These frameworks and plans should:
   - prioritise information technology systems recovery in the event of a disaster impacting a number of departments and agencies
   - cover financial and non-financial systems.

4 Focus areas 2014–15

At a glance

Background

In 2014–15 we had two focus areas:

- identity and access management (IDAM) controls—controls which aim to reduce the risk of inappropriate access to information and data
- software licensing controls—controls implemented to manage the purchasing and deployment of software and ongoing compliance throughout its use. Effective management of software licences reduces the risks of breaching software licence contracts, aims to maximise volume pricing and reduce redundant purchasing.

Conclusion

IDAM controls at more than half of the 30 in-scope entities require improvement. While software licensing is generally well-managed across the in-scope entities, there are a number of opportunities for improvement.

Findings

IDAM controls in the areas of assurance and authentication controls, user access management and ongoing monitoring are not sufficiently mature at more than half of the in-scope entities.

Software licensing controls, in particular key controls which restrict the installation of software by end-users, were generally found to be established and mature for in-scope entities. Software licensing policies and procedures, and compliance monitoring, however, requires improvement at more than half of the in-scope entities.

Recommendations

That public sector entities' governing bodies and management:

- enhance identity and access management, and software licensing policies and procedures by addressing control weaknesses reported in management letters
- implement processes to periodically monitor the effectiveness of identity and access management, and software licensing processes and controls.

4.1 Introduction

As outlined in our *Annual Plan 2014–15*, this report analysed two areas of focus:

- identity and access management (IDAM)
- software licensing.

IDAM relates to how individuals are provided with an appropriate level of access to data and information. The government-wide adoption of common policy, standards, guidelines and processes for IDAM enables the Victorian Government to reduce the risk of inappropriate information release or access.

A software licence is a contract with a software publisher or copyright holder that includes the terms under which the user may install, use, copy, modify or distribute the software. In effect, users are entering into an agreement to use a licensed product for a fee, subject to the terms and conditions of the software licence. The *Copyright Act 1968* provides legal protection for the intellectual property rights of software developers and licensed distributors of software. Under the *Copyright Act 1968*, it is generally an infringement to copy software without the permission of the copyright owner.

A total of 30 entities—from the 45 selected for this report—were surveyed using questionnaires. These entities are detailed in Appendix B. The questionnaires were completed as part of our financial audit information technology (IT) audit fieldwork and where appropriate, the audit team requested supporting evidence and challenged the assertions made by management.

The result of our analysis of the two focus areas was communicated to management as part of our audit. Our assessment is summarised using the following ratings, which are used in all the figures in this Part.

Rating	Description
	Key controls are established and processes are mature.
	Key controls are established but underlying processes are not sufficiently mature. Exceptions in processes are still noted but not widespread.
	Key controls and a systematic process are absent.

4.2 Identity and access management

4.2.1 Introduction

When assessing IDAM controls we considered the following five sub-areas:

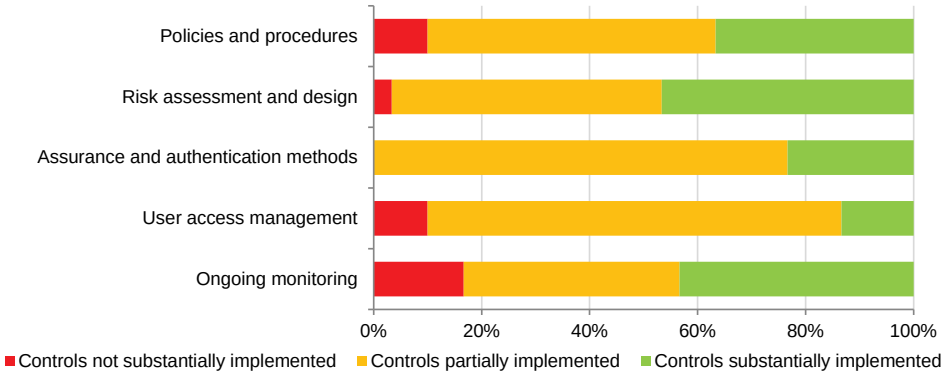
- **IDAM policies and procedures**—entity-wide IDAM frameworks that govern information classification, access and authentication. Includes how these frameworks consider and align with applicable guidance and better practices, such as the Victorian Government IT security standards, the Commonwealth's *National e-Authentication Framework* and the *Australian Government Information Security Manual*.

- **Risk assessment and design of IDAM**—the awareness of the entity's IDAM controls and existing gaps. Also examines, at a high level, how IDAM processes are integrated with human resources processes and technological enablers, such as single sign on and identity management systems, to ensure consistency of controls across the entity.
- **Assurance and authentication controls**—examines how authentication to systems is designed and if it is based on risk factors. Considers the strength of the authentication controls and whether management had considered the appropriate use of 'two-factor' authentication or 'one-time use passwords' for access that may entail higher risks. Two-factor authentication includes something the user knows—i.e. a password—and something the user has—i.e. a security token. One-time use passwords are valid for only one login session or transaction.
- **User access management**—processes designed to ensure a user's access to systems is aligned with the user's business need and the principles of 'segregation of duties'. Considers the processes and controls throughout the user access lifecycle, including creating a new user, modifying their access and removing their access.
- **Ongoing monitoring**—processes designed to ensure that IDAM remains a robust and monitored activity. It also examines how the entities existing frameworks are monitored to ensure they remain aligned with existing and upcoming frameworks and guidance.

4.2.2 IDAM audit findings

IDAM was chosen as an area of focus due to the extent of audit findings in previous years in areas such as user access management and authentication controls. Government entities continue to have difficulties with these areas, increasing the risk that IT systems may be compromised, and potentially impacting the confidentiality and integrity of personal, sensitive and commercial information. Figure 4A summarises the results of our analysis of IDAM at the 30 in-scope entities.

Figure 4A
IDAM focus area results



Source: Victorian Auditor-General's Office.

IDAM policies and procedures

Half of the 30 in-scope entities had policies or procedures which were fit-for-purpose and sufficiently detailed to guide better practice in areas such as system access, user management and password controls. The remaining entities needed to update their policies and procedures, or include absent controls.

Risk assessment and design of IDAM

IDAM requirements are driven by a number of considerations, usually a combination of better practice guidance and internal risk assessments.

Half of the 30 in-scope entities had some human resource processes integrated with existing IDAM processes and systems. The remaining entities have either partially integrated or not integrated their processes, and therefore undertake a relatively manual process. The use of 'single sign-on' software to manage access to internal systems is widespread and is commonly cited as a key tool in managing user access.

User access management, and assurance and authentication controls

User access management and assurance and authentication controls are included within the scope of our IT audits, and therefore are reported on in Part 3 of this report.

The majority of the 30 in-scope entities are not enforcing appropriate user access management or assurance and authentication controls. Specifically:

- 20 of the 30 in-scope entities had audit findings relating to authentication related controls, usually passwords
- 23 of the 30 in-scope entities had audit findings relating to the management of user access.

Ongoing monitoring

Forty-seven per cent of in-scope entities had processes in place to periodically:

- review the IDAM framework and policies for alignment with applicable standards or better practices
- monitor the entity's IT environment for compliance with the IDAM framework.

The remaining 53 per cent of entities had audit findings reported in relation to either:

- the frequency of their updates to internal frameworks and policies, and their lack of consideration of Victorian Government IT security standards
- not having a program in place to monitor compliance with IDAM frameworks, or not retaining evidence to demonstrate the effectiveness of this program.

4.2.3 Top four sector results

The characteristics of the top four sectors are described in Part 3 of this report. Entities within the top four sectors account for 80 per cent of 30 entities examined in this Part.

Environment and water

Figure 4B summarises our assessment of IDAM at the eight in-scope environment and water entities.

Figure 4B
IDAM in the environment and water sector

	Environment and water entity							
IDAM sub-area	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
IDAM policies and procedures	●	●	●	●	●	●	●	●
Risk assessment and design of IDAM	●	●	●	●	●	●	●	●
Assurance and authentication methods	●	●	●	●	●	●	●	●
User access management	●	●	●	●	●	●	●	●
Ongoing monitoring	●	●	●	●	●	●	●	●

Source: Victorian Auditor-General's Office.

Consistent with the maturity assessment in Part 3 of this report, environment and water entities perform well when compared to other sectors. Most IDAM sub-areas are assessed to have no or minimal gaps and there are no sub-areas where key controls are systematically absent.

Areas requiring the most improvement in this sector are user access management and assurance and authentication methods.

Health and human services

Figure 4C summarises our assessment of IDAM at the five in-scope health and human services entities.

Figure 4C
IDAM in the health and human services sector

	Health and human services entity				
IDAM sub-area	**1**	**2**	**3**	**4**	**5**
IDAM policies and procedures	●	●	●	●	●
Risk assessment and design of IDAM	●	●	●	●	●
Assurance and authentication methods	●	●	●	●	●
User access management	●	●	●	●	●
Ongoing monitoring	●	●	●	●	●

Source: Victorian Auditor-General's Office.

IDAM controls within the health and human services sector are generally established but underlying processes are not sufficiently mature. With the exception of assurance and authentication controls, which were found to be generally effective, other IDAM sub-areas require improvement. There are no sub-areas where key controls and systematic process are not present.

Only one in-scope entity had three sub-areas for which controls were rated as established and mature. Controls over access management and ongoing monitoring assessed as only partially implemented across all in-scope entities.

Departments and central agencies

Figure 4D summarises our assessment of IDAM at the eight in-scope departments and central agencies.

Figure 4D
IDAM in departments and central agencies

	Departments and central agencies entity							
IDAM sub-area	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
IDAM policies and procedures	●	●	●	●	●	●	●	●
Risk assessment and design of IDAM	●	●	●	●	●	●	●	●
Assurance and authentication methods	●	●	●	●	●	●	●	●
User access management	●	●	●	●	●	●	●	●
Ongoing monitoring	●	●	●	●	●	●	●	●

Source: Victorian Auditor-General's Office.

IDAM controls within in-scope departments and central agencies are mostly established but underlying processes still require improvement.

Seven of the eight in-scope entities have user access management and assurance and authentication controls that require improvement. This is due to a shared service arrangement with a common IT service provider. The only entity that was rated as having established and mature controls in these sub-areas does not depend on this shared service provider for its key IDAM controls. Improvements to this shared service provider's controls would be felt across all these entities.

IDAM policies and procedures and ongoing monitoring were absent at one in-scope entity.

Justice

Figure 4E summarises our assessment of IDAM at the three in-scope justice entities.

Figure 4E
IDAM in the justice sector

	Justice entity		
IDAM sub-area	**1**	**2**	**3**
IDAM policies and procedures	●	●	●
Risk assessment and design of IDAM	●	●	●
Assurance and authentication methods	●	●	●
User access management	●	●	●
Ongoing monitoring	●	●	●

Source: Victorian Auditor-General's Office.

Consistent with the maturity assessment in Part 3 of this report, justice entities perform relatively poorly when compared to other sectors. In a number of sub-areas, key controls are absent or ineffective. Notably, ongoing monitoring controls are lacking across all the justice sector in-scope entities, reflecting a low level of internal awareness of IDAM gaps.

No in-scope justice agency has any key IDAM controls which are established and mature. Coming from this relatively lower base, there is a significant opportunity for these entities to improve their performance in the future.

4.3 Software licensing

4.3.1 Introduction

When assessing software licensing controls we considered the following four sub-areas:

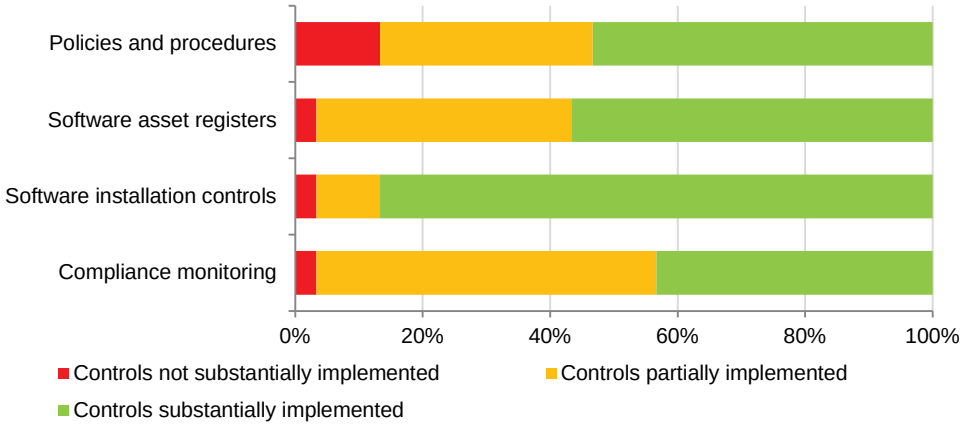
- **software licensing policies and procedures**—policies and procedures governing authorised software use and licensing. Also includes clarity of roles and responsibilities and internal processes. Outlines the scope of software covered.
- **software asset registers**—the management and ongoing maintenance of software asset registers. *Standing Directions of the Minister for Finance under the Financial Management Act 1994* (Standing Directions) indicate that a 'register of licences for financial management software must be maintained'.
- **software installation controls**—controls to minimise the use of unauthorised software within the IT environment. This may include controls such as a 'locked desktop' which restricts the installation of software by end-users.

- **compliance monitoring**—managements assessments of the entities software licensing compliance, including the use of tools. Standing Directions state that 'regular audits or verification reviews of the [software] register must be performed (at least annually)'.

4.3.2 Software licensing audit findings

Figure 4F summarises the results of our analysis of software licensing controls at the 30 in-scope entities.

Figure 4F
Software licensing focus area results



Source: Victorian Auditor-General's Office.

Software licensing policies, procedures and compliance monitoring

Sixteen of the 30 in-scope entities have formalised and documented software licensing policies and procedures. The remaining 14 entities:

- need to develop these documents
- have elements of software license management embedded within other documents
- need to update their documents to ensure they are current.

Despite the above, 83 per cent of entities have assigned the responsibility for managing software licensing to a staff member(s). This is reflected in that only one of the 30 in-scope entities did not have a software asset register and another one entity did not have any compliance monitoring controls.

Our assessment of compliance monitoring and asset register maintenance is mixed, showing that about half of the in-scope entities do these well.

Software asset registers

Thirteen of the 30 in-scope entities require improvements to their software asset registers. We found:

- instances of incomplete or missing software asset registers
- processes for updating asset registers were not documented
- a lack of evidence on the process for updating components of the software register.

Software installation controls

Twenty-seven of the 30 in-scope entities have implemented 'locked desktops' and standard operating environments to manage software deployments. At one of these entities we found an excessive number of 'local administrator' rights assigned to end-users. This level of access enables end-users to bypass the installation controls that had been implemented by management.

4.3.3 Top four sectors results

Environment and water

Figure 4G summarises our assessment of software licensing at the eight in-scope environment and water entities.

Figure 4G
Software licensing in the environment and water sector

	Environment and water entity							
Software licensing sub-area	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Software licensing policies and procedures	●	●	●	●	●	●	●	●
Software asset registers	●	●	●	●	●	●	●	●
Software installation controls	●	●	●	●	●	●	●	●
Compliance monitoring	●	●	●	●	●	●	●	●

Source: Victorian Auditor-General's Office.

Consistent with the maturity assessment in Part 3 of this report and the results of our assessment of IDAM, environment and water entities mostly have established software licensing controls and mature processes.

While two in-scope environment and water entities had been assessed as having partially implemented controls in three sub-areas, this was due to minor control gaps or a lack of clarity in roles and responsibilities.

Health and human services

Figure 4H summarises our assessment of software licensing at the five in-scope health and human services entities.

Figure 4H
Software licensing in the health and human services sector

	Health and human services entity				
Software licensing sub-area	**1**	**2**	**3**	**4**	**5**
Software licensing policies and procedures	●	●	●	●	●
Software asset registers	●	●	●	●	●
Software installation controls	●	●	●	●	●
Compliance monitoring	●	●	●	●	●

Source: Victorian Auditor-General's Office.

Figure 4H shows that:

- one in-scope health and human services entity has established controls and mature processes across all sub-areas—this is the same entity that had more effective IDAM processes and controls described in Part 3
- all in-scope health and human services entities had mature controls surrounding software installation
- areas for improvement included incomplete software registers, roles and responsibilities over compliance monitoring not being defined and a lack of software licensing policies and procedures.

Departments and central agencies

Figure 4I summarises our assessment of software licensing at the eight in-scope departments and central agencies.

Figure 4I
Software licensing in departments and central agencies

	Departments and central agencies							
Software licensing sub-area	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Software licensing policies and procedures	●	●	●	●	●	●	●	●
Software asset registers	●	●	●	●	●	●	●	●
Software installation controls	●	●	●	●	●	●	●	●
Compliance monitoring	●	●	●	●	●	●	●	●

Source: Victorian Auditor-General's Office.

The assessment of software licensing controls across departments and central agencies is varied. Two in-scope departments and central agencies have established controls and mature processes across all sub-areas. However, two other entities are lacking key controls and process in a number of sub-areas.

Key control weaknesses typically include:

- a lack of documented policies and procedures or roles and responsibilities
- incomplete software asset registers
- compliance monitoring not being performed or evidence of this not being retained.

Justice

Figure 4J summarises our assessment of software licensing at the three in-scope justice entities.

Figure 4J
Software licensing in the justice sector

	Justice entity		
Software licensing sub-area	**1**	**2**	**3**
Software licensing policies and procedures	●	●	●
Software asset registers	●	●	●
Software installation controls	●	●	●
Compliance monitoring	●	●	●

Source: Victorian Auditor-General's Office.

For two of the three in-scope justice entities, software licensing policies and procedures are inadequate and key controls are absent. One of these entities did not have a software licensing policy or procedure, while the other had a document that was last updated in 1994.

4.4 Challenges ahead

IDAM and software licensing control weaknesses at the 30 in-scope entities all relate to the lack of:

- clearly defined expectations in the form of policies and procedures
- well-defined accountabilities and responsibilities
- awareness of the control weaknesses.

Where there is limited visibility or clarity on activities and controls, either internal or external, there is a higher chance of controls being neglected or being performed in an ineffective manner. For example, where software asset registers are decentralised and maintained by teams in different business units across an entity, key activities may differ. Centralising this activity to an appropriate team or staff member, and providing clear guidelines and periodic audits, would improve the quality of information within the asset registers.

An example relating to IDAM is the process in place between the departments and its IT service provider, where activities are either outsourced or jointly managed. In our audits, we noted there some controls operating but without a clear understanding of what the other parts of the entity are doing, creating inefficiencies and ineffectiveness. In some cases, it was assumed that the other party was acting in a particular capacity or on a particular task when this was not the case. To compound the problem, these processes are managed through multiple disjointed systems, with processes varying slightly varying between different teams. Harmonising controls into a single system and process would require cooperation from all parties.

Recommendations

That public sector entities' governing bodies and management:

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.

Appendix A.
Rating definitions

Ratings for audit findings reflect our assessment of both the likelihood and consequence of each identified issue in terms of its impact on:

- the effectiveness and efficiency of operations, including probity, propriety and compliance with applicable laws
- the reliability, accuracy and timeliness of financial reporting.

The ratings also assist management to prioritise remedial action.

Figure A1
Rating definitions and management action

Rating	Definition	Management action required
Extreme	The issue represents: • a control weakness which could cause or is causing severe disruption of the process or severe adverse effect on the ability to achieve process objectives and comply with relevant legislation	Requires immediate management intervention with a detailed action plan to be implemented within one month.
	or	
	• a material misstatement in the financial report has occurred.	Requires executive management to correct the material misstatement in the financial report as a matter of urgency to avoid a modified audit opinion.
High	The issue represents: • a control weakness which could have or is having a major adverse effect on the ability to achieve process objectives and comply with relevant legislation	Requires prompt management intervention with a detailed action plan implemented within two months.
	or	
	• a material misstatement in the financial report that is likely to occur.	Requires executive management to correct the material misstatement in the financial report to avoid a modified audit opinion.

Figure A1
Rating definitions and management action – *continued*

Rating	Definition	Management action required
Medium	The issue represents: • a control weakness which could have or is having a moderate adverse effect on the ability to achieve process objectives and comply with relevant legislation or • a misstatement in the financial report that is not material and has occurred.	Requires management intervention with a detailed action plan implemented within three to six months.
Low	The issue represents: • a minor control weakness with minimal but reportable impact on the ability to achieve process objectives and comply with relevant legislation or • a misstatement in the financial report that is likely to occur.	Requires management intervention with a detailed action plan implemented within six to 12 months.

Source: Victorian Auditor-General's Office.

Appendix B.

Financial systems controls report 2014–15: scope and coverage

Figure B1
Entities selected for this financial systems controls report

Entities	Scope details		
	Information technology (IT) audit	Focus areas	IT controls maturity assessment
Department and central agencies			
CenITex	[a]	Yes	Yes
Department of Economic Development, Jobs, Transport & Resources	Yes	Yes	Yes
Department of Education & Training	Yes[b]		
Department of Environment, Land, Water & Planning	Yes	Yes	Yes
Department of Health & Human Services	Yes	Yes	Yes
Department of Justice & Regulation	Yes	Yes	Yes
Department of Treasury & Finance	Yes	Yes	Yes
Department of Premier & Cabinet	Yes	Yes	Yes
State Revenue Office	[a]	Yes	Yes
State Trustees Limited	Yes[b]		
Environment and water			
Barwon Region Water Corporation	Yes[b]		
Central Gippsland Region Water Corporation	Yes	Yes	Yes
City West Water	Yes	Yes	Yes
Coliban Region Water Corporation	Yes	Yes	Yes
Goulburn-Murray Water	Yes	Yes	Yes
Grampians Wimmera Mallee Water	Yes[b]		
Melbourne Water Corporation	Yes	Yes	Yes
South East Water	Yes	Yes	Yes
Vicforests	Yes	Yes	Yes
Yarra Valley Water	Yes	Yes	Yes

Figure B1
Entities selected for this financial systems controls report – *continued*

Entities	Scope details		
	IT audit	Focus areas	IT controls maturity assessment
Health and human services			
Australian Health Practitioner Regulatory Agency	Yes		Yes
Ambulance Victoria	Yes		Yes
Ballarat Health Services	Yes	Yes	Yes
Barwon Health	Yes	Yes	Yes
Eastern Health	Yes[(b)]		
Monash Health	Yes	Yes	Yes
Peter MacCallum Cancer Centre	Yes	Yes	Yes
Royal Children's Hospital	Yes	Yes	Yes
Royal Women's Hospital	Yes		Yes
Justice			
Country Fire Authority	Yes	Yes	Yes
Court Services Victoria	Yes		
Metropolitan Fire Brigade	Yes	Yes	Yes
Victoria Police	Yes	Yes	Yes
Victorian Commission for Gambling and Liquor Regulation	Yes	Yes	
Victorian State Emergency Services	Yes		Yes
Economic development and transport			
Linking Melbourne Authority	Yes		
Museums Victoria	Yes[(b)]	Yes	
Places Victoria	Yes	Yes	Yes
Public Transport Victoria	Yes	Yes	Yes
Local government			
Ballarat City Council	Yes	Yes	Yes
City of Geelong	Yes[(b)]		
City of Melbourne	Yes	Yes	Yes
Mornington Peninsula Shire	Yes[(b)]		
Universities			
Deakin University	Yes		
Monash University	Yes		
Royal Melbourne Institute of Technology	Yes		
Swinburne University	Yes		

(a) Not a separate audited entity. Results of IT audit included under relevant department.

(b) Yes, limited scope audit, usually limited to a follow-up of the prior year's assessment or a high-level assessment of the IT environment.

Source: Victorian Auditor-General's Office.

Appendix C.

Audit Act 1994 section 16— submissions and comments

Introduction

In accordance with section 16(3) of the *Audit Act 1994*, a copy of this report was provided to the Department of Premier & Cabinet, the Commissioner for Privacy and Data Protection and Department of Environment Land, Water & Planning.

The submissions and comments provided are not subject to audit nor the evidentiary standards required to reach an audit conclusion. Responsibility for the accuracy, fairness and balance of those comments rests solely with the agency head.

Responses were received as follows:

RESPONSE provided by the Secretary, Department of Premier & Cabinet

Department of
Premier & Cabinet

1 Treasury Place
Melbourne Victoria 3002
Telephone: 03 9651 5111
dpc.vic.gov.au

D15/134366

RECEIVED
28 SEP 2015
VICTORIAN AUDITOR-GENERAL'S OFFICE

Dr Peter Frost
Acting Victorian Auditor-General
Level 24, 35 Collins Street
MELBOURNE VIC 3000

Dear Dr ~~Frost~~ pdv

Thank you for your letter of 17 September regarding the performance audit report *Financial systems controls report: Information technology 2014–15*.

I appreciate the opportunity to consider the report and its recommendations. My department shares your focus in ensuring appropriate policies and procedures are in place to preserve the confidentiality, integrity and availability of the government's IT systems and data.

We note recommendation 1 requires the Commissioner for Privacy and Data Protection to provide education and training to relevant entities on the requirements of the Victorian Government information technology standards.

Regarding recommendations 2 and 8, DPC will work with selected public service bodies to monitor and report on the status of information technology obsolescence risks, and the implementation of disaster recovery planning by shared services boards.

Recommendations 3–7 and 9 relate to public sector entities' governing bodies and management. DPC will develop action plans to implement these recommendations within the department, taking into account risk exposure and resourcing factors.

Yours sincerely

Chris Eccles
Secretary

Your details will be dealt with in accordance with the *Public Records Act 1973* and the *Privacy and Data Protection Act 2014*. Should you have any queries or wish to gain access to your personal information held by this department please contact our Privacy Officer at the above address.

State Government Victoria

RESPONSE provided by the Commissioner for Privacy and Data Protection

Commissioner
for Privacy and
Data Protection

01 OCT 2015

Ms Karen Phillips
Assistant Auditor-General, Information Systems Audit
Victorian Auditor-General's Office
Level 24, 35 Collins Street
MELBOURNE VIC 3000

Dear Ms Phillips

Financial Systems Control Report: Information Technology 2014-15

Recommendation number 1 of the draft Financial Systems Control Report obliges my office to provide education and training to relevant entities on the requirements of the Victorian Protective Data Security Standards, when issued.

I am pleased to advise that I accept this recommendation, with the understanding that the relevant entities are those within the jurisdiction of Part 4 of the *Privacy and Data Protection Act 2014*.

I envisage at this stage that the Victorian Protective Data Security Standards will be issued on 1 January 2016.

Yours sincerely,

DAVID WATTS
Commissioner for Privacy and Data Protection

Commissioner for Privacy and Data Protection
PO BOX 24014, MELBOURNE VIC 3001 T +61 3 8684 1660 W cpdp.vic.gov.au E enquiries@cpdp.vic.gov.au

VICTORIA State Government

RESPONSE provided the Secretary, Department of Environment Land, Water & Planning

Department of Environment
Land, Water & Planning

8 Nicholson Street
East Melbourne, Victoria 3002
PO Box 500
East Melbourne, Victoria 8002
www.delwp.vic.gov.au

Ref: SBR008136

RECEIVED
28 SEP 2015
VICTORIAN AUDITOR-GENERAL'S OFFICE

Mr Peter Frost
Deputy Auditor-General
Level 24, 35 Collins Street
Melbourne Vic 3000

Dear Mr Frost

PROPOSED VAGO AUDIT REPORT - FINANCIAL SYSTEMS CONTROLS REPORT 2014-15: INFORMATION TECHNOLOGY

Thank you for your letter dated 17 September 2015 providing the opportunity to comment on the proposed audit report *Financial systems controls report 2014-15: Information Technology*.

The Department of Environment, Land, Water and Planning (DELWP) is committed to ensuring that its information technology financial controls are managed within acceptable risk tolerances. The department welcomes the findings in the report and accepts the recommendations directed at the public sector entities.

I am also pleased to advise that specific issues relating to DELWP reported in the interim and final management letters issued by your office have been registered in the department's audit action tracking system and will be monitored and actioned in accordance with the department's internal procedures.

Thank you for the opportunity to comment on the report.

Yours sincerely

Paul Smith
Acting Secretary

24 SEP 2015

Any personal information about you or a third party in your correspondence will be protected under the provisions of the *Privacy and Data Protection Act 2014*. It will only be used or disclosed to appropriate Ministerial, Statutory Authority, or departmental staff in regard to the purpose for which it was provided, unless required or authorized by law. Enquiries about access to information about you held by the Department should be directed to the Privacy Coordinator, Department of Environment, Land, Water and Planning, PO Box 500, East Melbourne, Victoria 8002.

VICTORIA State Government

Auditor-General's reports

Reports tabled during 2015–16

Report title	Date tabled
Follow up of Collections Management in Cultural Agencies (2015–16:1)	August 2015
Follow up of Managing Major Project (2015–16:2)	August 2015
Follow up of Management of Staff Occupational Health and Safety in Public Schools (2015–16:3)	August 2015
Biosecurity: Livestock (2015–16:4)	August 2015
Applying the High Value High Risk Process to Unsolicited Proposals (2015–16:5)	August 2015
Unconventional Gas: Managing Risks and Impacts (2015–16:6)	August 2015
Regional Growth Fund: Outcomes and Learnings (2015–16:7)	September 2015
Realising the Benefits of Smart Meters (2015–16:8)	September 2015
Delivering Services to Citizens and Consumers via Devices of Personal Choice: Phase 2 (2015–16:9)	October 2015

VAGO's website at www.audit.vic.gov.au contains a comprehensive list of all reports issued by VAGO.

VAGO
Victorian Auditor-General's Office
Auditing in the Public Interest

Availability of reports

All reports are available for download in PDF and HTML format on our website www.audit.vic.gov.au

Victorian Auditor-General's Office
Level 24, 35 Collins Street
Melbourne Vic. 3000
AUSTRALIA

Phone: +61 3 8601 7000
Fax: +61 3 8601 7010
Email: comments@audit.vic.gov.au