Information and Communications Technology Controls Report 2013–14

Victorian Auditor-General's Report | October 2014 | 2014–15:12

VICTORIA

Victorian
Auditor-General

Information and Communications Technology Controls Report 2013–14

Ordered to be printed

VICTORIAN
GOVERNMENT PRINTER
October 2014

PP No 380, Session 2010–14

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 03 4

VAGO

Victorian Auditor-General's Office

Auditing in the Public Interest

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

The Hon. Christine Fyffe MP
Speaker
Legislative Assembly
Parliament House
Melbourne

Dear Presiding Officers

Under the provisions of section 16AB of the *Audit Act 1994*, I transmit my report *Information and Communications Technology Controls Report 2013–14*.

This report is the first of its type by my office and aims to provide additional insight and increase visibility of ICT-related audit findings, raised as part of our 2013–14 financial audits. The report is intended to provide decision-makers with relevant information to assist them to address audit findings and improve processes.

For this audit, 39 entities with a financial year-end date of either 31 December 2013 or 30 June 2014 were selected for analysis. Sixty-four key financial ICT applications and their infrastructure were audited, with 364 associated audit findings used as the basis for this report's analysis.

Most ICT audit findings were medium risk, with none ranked as an extreme risk. High-risk ICT audit findings are concentrated in a few ICT general controls categories. This report also draws out five clear emerging themes from the analysis and I have made seven recommendations to help address these.

In future reports, we will perform detailed maturity assessments of selected entities' ICT environments and also examine some selected areas of focus, such as identity and access management, software licensing and wireless network security.

Yours faithfully

John Doyle
Auditor-General

15 October 2014

Contents

Auditor-General's comments

John Doyle
Auditor-General

My office undertakes a number of information and communications technology (ICT) audits each financial year to verify whether key financial ICT systems are managed appropriately to support the financial reporting process.

Reflecting on the 364 ICT audit findings relevant to the 39 entities selected for this inaugural report, I see a number of key issues that require much more focused attention and oversight by accountable officers and governance bodies.

Overwhelmingly, a recurring finding is the need to improve ICT security controls. Inadequate management of ICT security accounts for a large proportion of the ICT audit findings reported during our financial audits.

Software patch management and ICT disaster recovery planning are also areas which require urgent attention.

Disappointingly, some 45 per cent of audit findings from previous years are yet to be rectified. Agencies need to accelerate the rate at which they are resolving audit findings and make sure that their underlying processes are improved so that audit findings do not re-occur.

Agencies seem to be having more success at addressing low-risk ICT audit findings compared to medium- and high-risk findings. This may be correlated with the degree of effort that is required in driving appropriate actions, but also raises questions about how audit recommendations are prioritised, tracked and monitored by management and key governance bodies, such as audit committees.

Consequently, I will be closely monitoring agencies' progress in the implementation of audit recommendations in future iterations of this ICT controls report.

Looking to the future, the growth of ICT outsourcing to the private sector and adoption of cloud-based ICT services is a trend that is likely to continue. While there may be many potential benefits from these services, the risks associated with such an approach need to be understood and actively managed by entities that are taking up such arrangements.

I would like to thank the participating agencies for their assistance and cooperation during the preparation of this audit.

John Doyle
Auditor-General

October 2014

Audit team

Paul O'Connor
Engagement Leader

Ian Yaw
Team Leader

Rue Maharaj
Team Member

Tonderai Nduru
Team Member

Engagement Quality Control Reviewer

Paul Martin

Audit summary

This report summarises the results of our audits of selected public sector entities' information and communication technology (ICT) general controls performed in support of VAGO's 2013–14 financial audits. ICT general controls are policies, procedures and activities put in place by an entity to assist and maintain the confidentiality, integrity and availability of its ICT systems and data.

This report is the first of its type and aims to provide additional insight and increase visibility of our ICT audit findings. This report is also intended to provide decision-makers with relevant information to assist them to address audit findings, and improve processes, and to enhance accountability across government.

For this audit, 39 entities with a financial year-end date of either 31 December 2013 or 30 June 2014 were selected for analysis. The audit findings of 64 ICT applications relevant to financial reporting and associated infrastructure are analysed in this report.

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

Conclusions

Despite some deficiencies in ICT controls, VAGO was able to rely on them for financial reporting purposes, as satisfactory mitigations had been identified and tested.

Most of the ICT audit findings were in the medium-risk category, with none ranked as an extreme risk. High-risk ICT audit findings are concentrated in a few ICT general controls categories.

For the 2013–14 financial year, there are five clear emerging themes or trends.

Findings

High-risk ICT audit findings are concentrated around deficiencies in controls for:

- managing access to ICT applications and data
- assurance obtained by entities over ICT general controls performed by external organisations
- entities using ICT systems, which are no longer supported by vendors
- authenticating users to ICT systems, such as password controls
- software patch management, such as implementing software releases by vendors to fix security vulnerabilities or operational issues
- maintaining processes to assist in the recovery of an entity's ICT in the event of a disaster.

Collectively, these findings account for 87 per cent of all high-risk findings.

Based on our analysis of the ICT audit findings, we identified the following top five themes:

- **ICT security controls need improvement**—ICT security audit findings account for the majority of all audit findings reported in the 2013–14 financial year. Further analysis shows that such audit findings are widespread across government, with VAGO reporting ICT security audit findings at most of the audited agencies.
- **Management of service organisation assurance activities requires attention**—in the context of this report, service organisations are ICT service providers, data processing services and external investment managers, with the state's ICT shared services body, CenITex, being an example of such an arrangement. Where such organisations have control over key ICT processes, VAGO would seek to obtain a service assurance report that articulates the effective control environment. There is an increase in the number of service assurance reports and similar instruments being obtained by public sector entities. It is likely that management's and VAGO's reliance on such reports will continue given the government's goal to outsource CenITex and for entities to consider using cloud-based applications.
- **Prior-period audit findings are not being addressed in a timely manner**—a number of weaknesses in ICT general controls raised in prior years have not been completely resolved by entities, despite agreement and commitment by management to resolve them.
- **Patch management processes need improvement**—most of the audited agencies have audit findings relating to patch management. Of the ICT general controls categories, patch management is ranked the lowest in terms of maturity, reflecting a need for management to improve their processes in this area.
- **ICT disaster recovery planning is weak**—a number of high-risk findings were highlighted in our audit reports. Most notable is an audit finding for one of the key providers for ICT services which relates to the absence of a formalised disaster recovery plan and framework and limited capability to respond to a significant ICT disaster.

Recommendations

Number	Recommendation	Page
Noting the high-level findings, public sector entities—governing bodies and management—and the Department of State Development, Business and Innovation, should:		
1.	enforce information and communication technology security policies and procedures, including improving user access management, authentication controls and patch management processes	38
2.	develop and implement appropriate policy and guidance on assurance activities surrounding outsourced information and communication technology arrangements	38
3.	enhance their understanding of the Assurance or Auditing Standards requirements for service assurance reports, ensure that reports received are fit for purpose and provide an accurate reflection of the control environment	38
4.	implement actions to address control weaknesses in outsourced information and communication technology arrangements	38
5.	implement sustainable process improvements to prevent re-occurring audit findings	38
6.	through audit committees, implement appropriate monitoring mechanisms to ensure audit findings are addressed by management	38
7.	develop appropriate information and communication technology disaster recovery capabilities, involving information and communication technology service providers as necessary.	38

Submissions and comments received

We have engaged with the Chief Technology Advocate within the Department of State Development, Business and Innovation 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 Department of State Development, Business and Innovation 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

The Auditor-General is the external auditor of Victoria's public sector entities, and has a legislated obligation to provide independent assurance to the Parliament about the financial status as well as efficiency, effectiveness and economy of these entities.

VAGO audits around 550 entities, including departments and agencies, public hospitals and other health services, universities and other educational institutions, water authorities, public sector superannuation funds, as well as companies, trusts and joint ventures controlled by public sector agencies.

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

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

This report summarises the results of our audits of public sector entities' ICT general controls as part of the 2013–14 financial audits. It is the first report of its type and aims to provide extra insight into VAGO's ICT audit findings, and identify wider trends that may not be covered in reports to an entity's management.

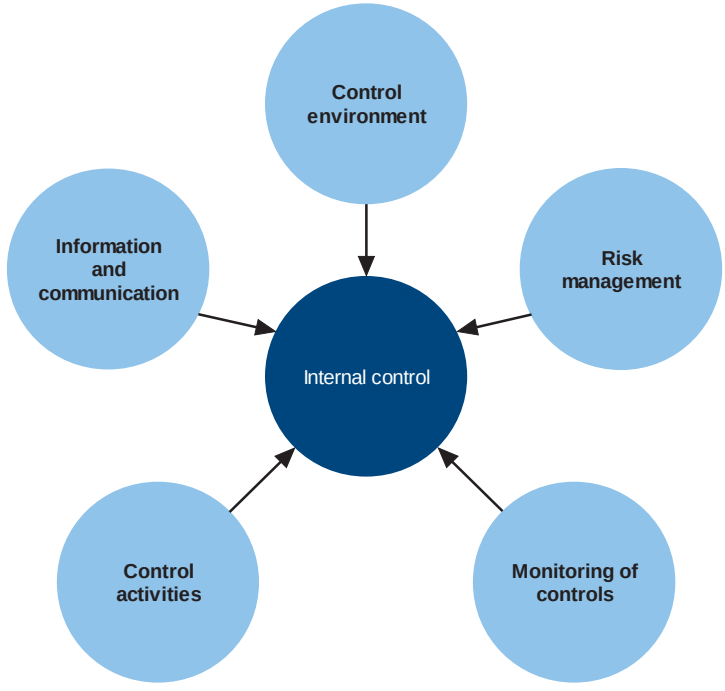
In future reports, we will perform detailed maturity assessments of selected entities' ICT environments and examine some selected areas of focus, such as identity and access management, software licensing and wireless network security.

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 its 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. 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. 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 ICT systems to initiate and process transactions, the ICT system is the sole repository of the documentation for financial transactions. A significant internal control weakness in the ICT 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.

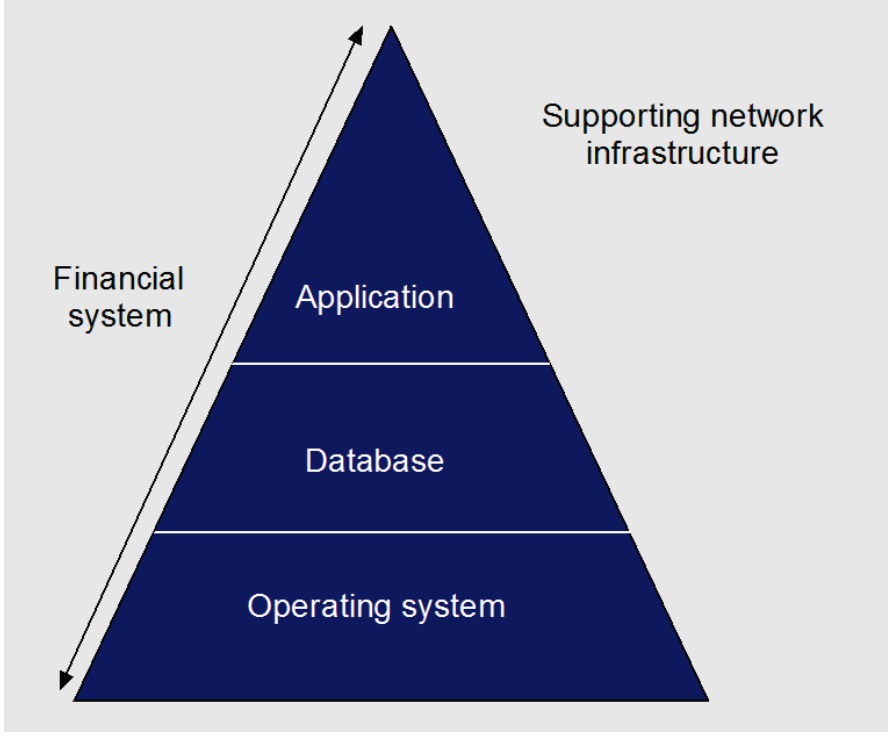
The importance of ICT systems and ICT general controls

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

- **Operating system**—core programs that run on the ICT 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 Oracle database and Microsoft SQL Server.
- **Applications**—programs that deliver operational or business requirements. There are various types of ICT applications, which are described in Section 1.5.

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

Figure 1B
Typical scope for an ICT general controls audit



Source: Victorian Auditor-General's Office.

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

Auditing Standard ASA 315 *Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment* states that ICT 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 ICT general control is whether access requests to ICT systems are properly reviewed and authorised by management. The objective of this control is to ensure only authorised users have access to entities' ICT systems.

Ineffective ICT 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 ICT 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 ICT audits.

Machinery-of-government changes

Machinery-of-government changes were announced in April 2013, culminating in a restructuring of departments early in the 2013–14 financial year.

The changes affected a number of key departments. From an ICT perspective, most notable was the restructure of the former Department of Business and Innovation to form the Department of State Development, Business and Innovation (DSDBI), along with newly assigned responsibilities for public sector ICT strategy, policy, and operations.

Given its role for ICT matters with government, VAGO consulted with DSDBI as the lead agency for this report.

CenITex

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

CenITex provides ICT infrastructure and services to DSDBI, as well as the departments of Environment and Primary Industries, Health, Human Services, Justice, Premier and Cabinet, Transport, Planning and Local Infrastructure, Treasury and Finance, some of these departments' associated agencies, as well as the Environment Protection Authority, Public Transport Victoria and Court Services Victoria.

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

The *Securing Victoria's Economy* statement of December 2012 and the *Victorian Government ICT Strategy* of February 2013—updated in March 2014—expressed an aim to enable more efficient and effective use of ICT across government by leveraging available private sector services.

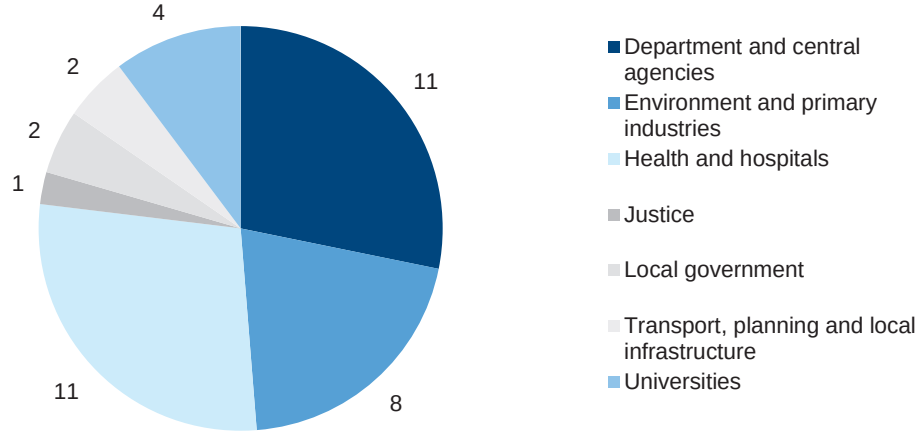
This policy approach aims to transition CenITex services to private sector contracts. To achieve this outcome, the government initiated Program Evolve, which was transferred from CenITex to DSDBI on 1 July 2014.

1.4 Departments and agencies in scope

This report summarises the results of the audits of ICT general controls conducted as part of the annual financial audits of 39 selected entities, with a financial year-end date of either 31 December 2013 or 30 June 2014—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



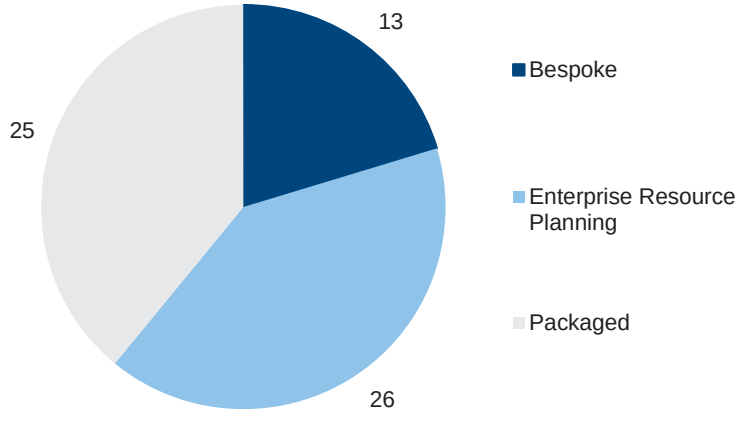
Note: For the purposes of this report, departments are grouped with other central agencies and described as 'Departments and central agencies'.
Source: Victorian Auditor-General's Office.

1.5 ICT systems in scope

Within the 39 selected entities, we audited the ICT general controls relating to 64 ICT applications and associated ICT infrastructure. These applications are a combination of financial and operational applications that support key financial processes.

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

Figure 1D
In-scope ICT applications by type



Source: Victorian Auditor-General's Office.

A description of the ICT 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 ICT 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 ICT 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 articulates 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 is used to support controls, and can be relied upon over key processes and cycles, 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 39 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 $144 000.

1.8 Structure of the report

The remainder of this report is structured as follows:

- Part 2 provides a summary of the ICT audit findings noted as part of the 2013–14 audits.
- Part 3 examines the top five themes or trends noted during the course of the ICT audits.

2 Results of ICT audits

At a glance

Background

For the 39 selected entities in scope for this report, we prepared management letters to bring to the entity's attention any identified control weaknesses from our information and communications technology (ICT) audits. For this report, these management letters were analysed to allow comment on issues and to identify any overarching themes that may have a broader impact.

Conclusion

Despite some deficiencies in ICT controls, VAGO was able to rely on controls for financial reporting purposes, as satisfactory mitigations had been identified and tested.

Most of the ICT audit findings were in the medium-risk category, with none rated as extreme risk.

Findings

- User access management and authentication controls are weak and account for the most frequent high-risk findings, highlighting the need for improvements in this area.
- Other prominent high-risk ICT audit findings identified related to:
  - 'other' ICT general controls categories, namely, third party assurance and high-risk systems end-of-life
  - patch management
  - backup management, business continuity and ICT disaster recovery planning.

2.1 Introduction

This Part analyses, at a high level, the outputs from our information communications technology (ICT) general controls audits conducted as part of the 2013–14 financial audits.

The audit findings were analysed according to:

- **risk rating**—the ratings are Extreme, High, Medium and Low. The ratings are explained in Section 2.2, with further detail in Appendix A.
- **ICT general controls category**—for example, user access management.

These audit findings were also used for our maturity assessment of the ICT controls environment, and are detailed in Section 2.4.

2.2 2013–14 ICT general controls audits results

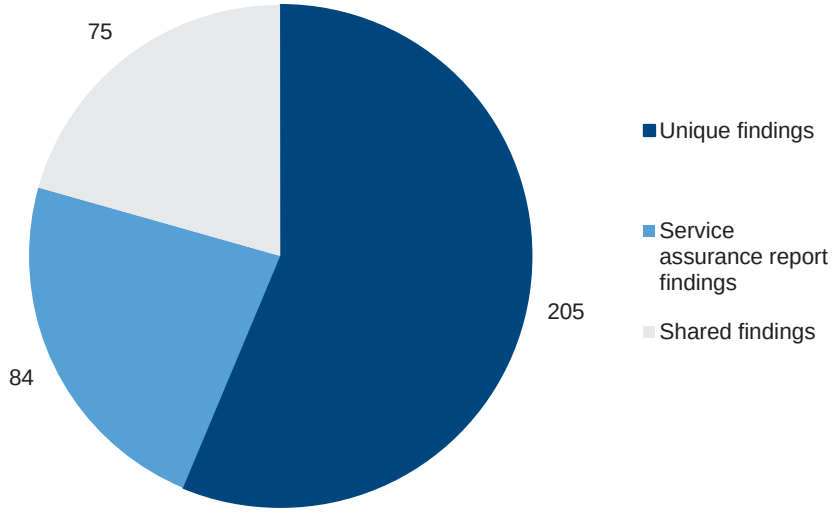
Overview of ICT audit findings

For the 39 selected entities for the 2013–14 financial year, 364 new and previously identified ICT audit findings were reported.

As shown in Figure 2A, of these audit findings:

- 75 were shared findings as a result of ICT environments being shared across entities
- 84 were identified from outsourced ICT service assurance reports.

Figure 2A
Total new and prior-year audit findings not addressed



Source: Victorian Auditor-General's Office.

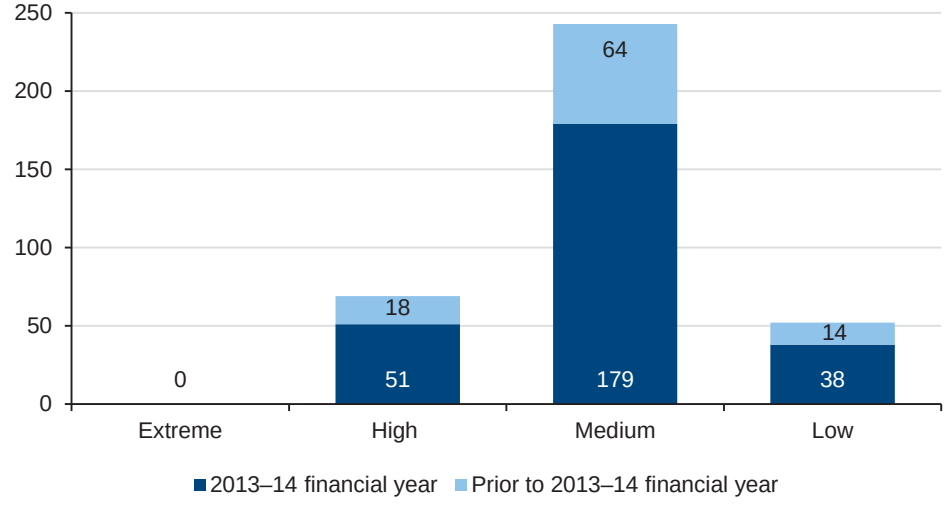
Of the audit findings, 77 per cent relate to VAGO's ICT audits of the in-scope entities, with the remaining 23 per cent relating to the outsourced ICT service assurance reports. Further insights into these outsourced ICT service assurance engagements are in Part 3.

ICT audit findings by risk rating

All our ICT audit findings are given 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.

Figure 2B show an analysis of findings by risk rating and whether the findings were new or prior-year findings.

Figure 2B
Findings by risk rating—new and prior year audit findings not addressed



Source: Victorian Auditor-General's Office.

ICT audit findings by category

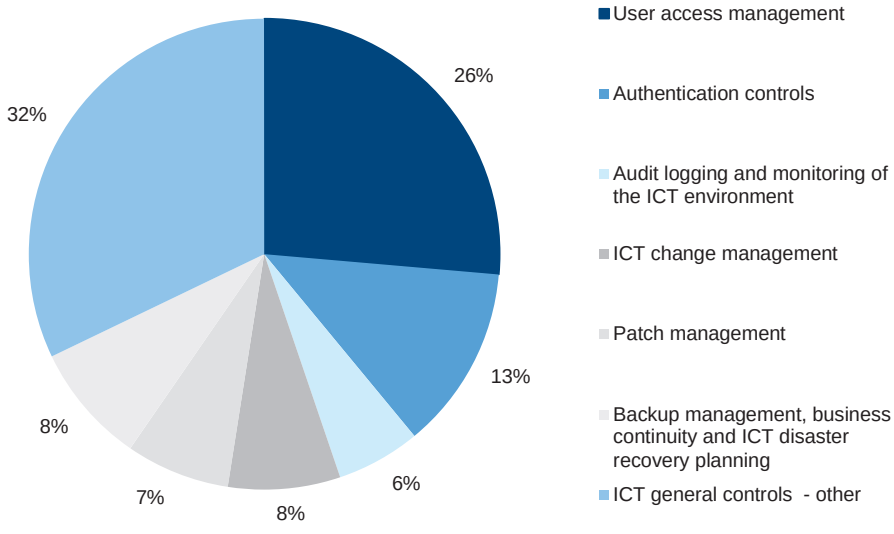
Financial audit procedures—including the need to understand and evaluate an entity's ICT environment and general controls—are risk based. ICT general controls commonly reviewed by VAGO as part of the financial audit are summarised into the following categories:

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

'Other' ICT general controls are a collection of findings that do not necessarily correspond with the above groups.

Figure 2C highlights the percentage of ICT audit findings identified by category.

Figure 2C
Percentage of findings by ICT general controls category



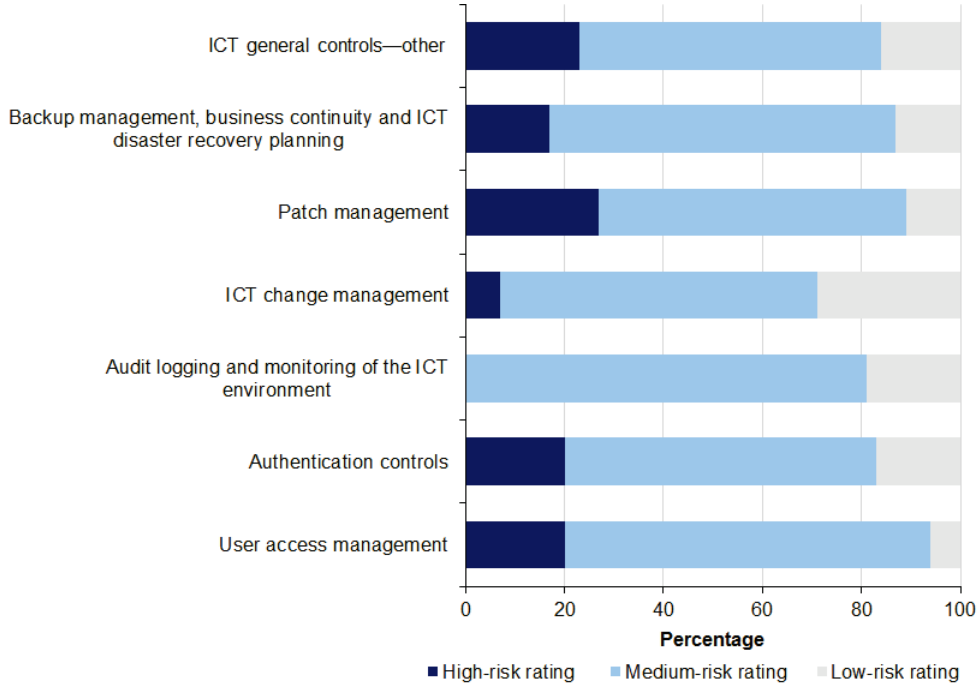
Source: Victorian Auditor-General's Office.

ICT audit findings by category and risk

As shown in Figure 2D, high-risk ICT audit findings are concentrated around the following ICT general control categories—accounting for 87 per cent of all high-risk findings:

- user access management
- 'other' ICT general controls categories–third party assurance and systems end-of-life
- authentication controls
- patch management
- backup management, business continuity and ICT disaster recovery planning.

Figure 2D
Distribution percentages of audit findings by risk ratings



Source: Victorian Auditor-General's Office.

2.3 ICT general controls categories

2.3.1 User access management

Description of the ICT general controls category

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.

This area also involves a review of appropriateness of 'super users', or users who have wide-ranging authorisation within applications and systems, including the creation of other regular and super users. User access management's primary objective is to maintain the confidentiality and integrity of ICT systems and data.

Why is this important?

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

Audit procedures performed

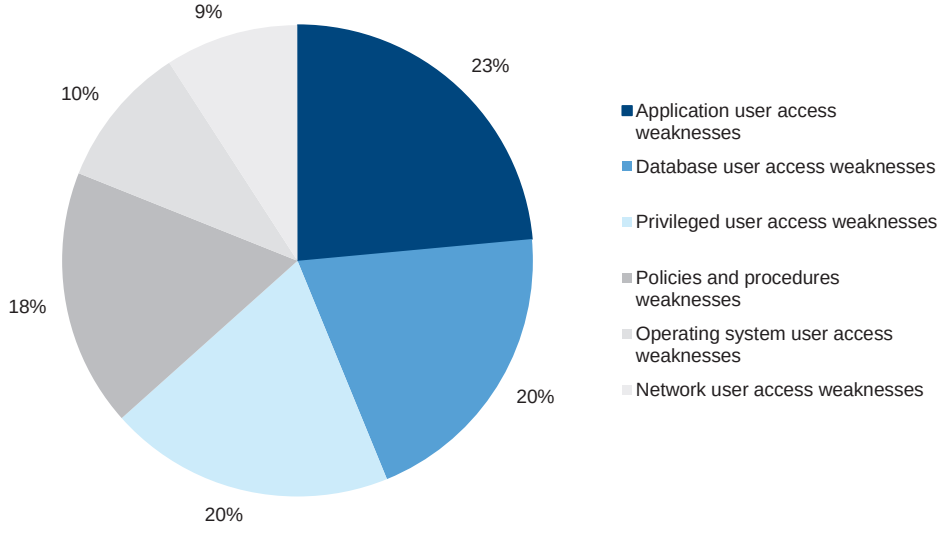
Our audit program examined the policies and procedures governing this process, as well as understanding and evaluating controls implemented by management to ensure access to systems and data is restricted to authorised users who require it for a legitimate business purposes.

Detailed analysis of audit findings

A total of 96 audit findings relating to user access management were reported in 2013–14, representing 27 per cent of total findings identified. User access management controls weaknesses accounted for 28 per cent of high-risk audit findings.

Figure 2E shows an even distribution of audit findings across the ICT environment—operating system, database and application—which suggests that improvements are required at all levels.

Figure 2E
User access management audit findings



Source: Victorian Auditor-General's Office.

Our analysis found that 82 per cent of the control weaknesses within user access management related to user account administration, which typically covers matters such as:

- inappropriate approval prior to access creation
- non-removal of user access upon termination
- non-review by management to ensure system access rights are aligned to a staff member's responsibilities.

A lower percentage of ICT audit findings in user access management related to policies and procedures, suggesting that these issues are mostly related to a lack of operational enforcement.

Excerpts of audit findings

Figure 2F gives examples of de-identified observations noted during ICT audits as part of 2013–14 financial audits.

Figure 2F
Typical user access management audit findings

- *80 accounts have been assigned super-user privileges to the <in-scope application> database server*
- *seven <vendor> staff have inappropriate SYSADMIN access to the <in-scope application>system*
- *periodic user access reviews have not been performed.*

Source: Victorian Auditor-General's Office.

2.3.2 Authentication controls

Description of the ICT general controls category

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

In ICT systems, 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.

Why is this important?

Weaknesses in authentication controls may lead to an increased risk that user account credentials could be compromised when passwords are not regularly changed, or are too easy to guess. This may lead to breaches in the confidentiality, integrity and availability of systems and data.

Audit procedures performed

Our audit program examined policies and procedures over password controls, as well as understanding and evaluating password controls implemented by management to restrict access to in-scope ICT applications and support infrastructure.

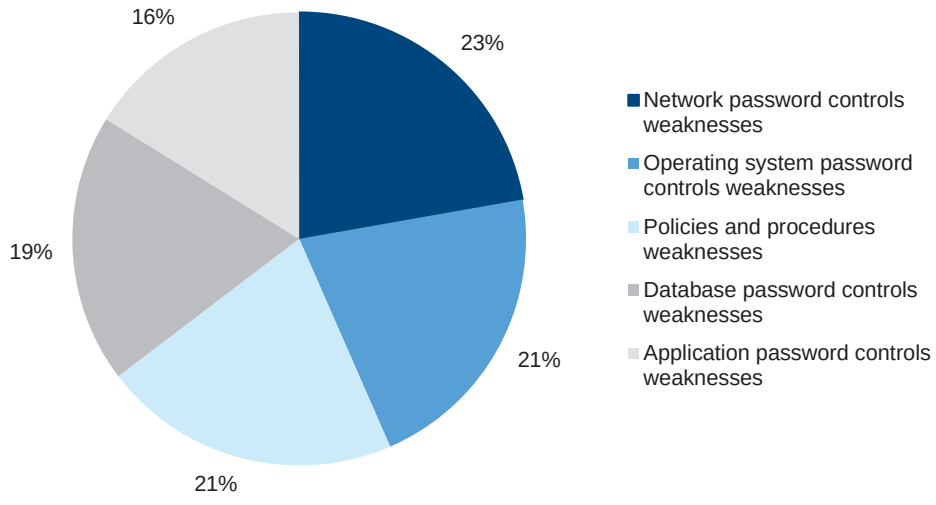
Detailed analysis of audit findings

Authentication controls weaknesses accounted for 46 audit findings, or 13 per cent, of the total findings identified. Weaknesses in authentication controls accounted for 13 per cent of high-risk audit findings.

As highlighted in Figure 2G, although there was a relatively high proportion of audit findings relating to policies and procedures, these findings do not necessarily reflect an absence of policies but rather a need to make existing policies more comprehensive to cover the full spectrum of password controls, such as database password controls and service accounts.

The audit findings are quite evenly distributed across the ICT environment—application, operating system, database and network.

Figure 2G
Authentication controls audit findings



Source: Victorian Auditor-General's Office.

Excerpts of audit findings

Figure 2H gives examples of de-identified observations noted during ICT audits as part of 2013–14 financial audits.

Figure 2H
Typical authentication controls audit findings

- *113 network user accounts have passwords that are configured to not expire. This includes five accounts assigned with super-user privileges to <organisation> network.*
- *Review of <in-scope system> password controls identified the following inappropriate configurations….*
- *Passwords to 79 <in-scope system> accounts have not been changed in a timely manner. The password ages range from 98 to 742 days.*

Source: Victorian Auditor-General's Office.

2.3.3 Audit logging and monitoring of the ICT environment

Description of the ICT general controls category

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

Why is this important?

Weaknesses in audit logging and monitoring of the ICT 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

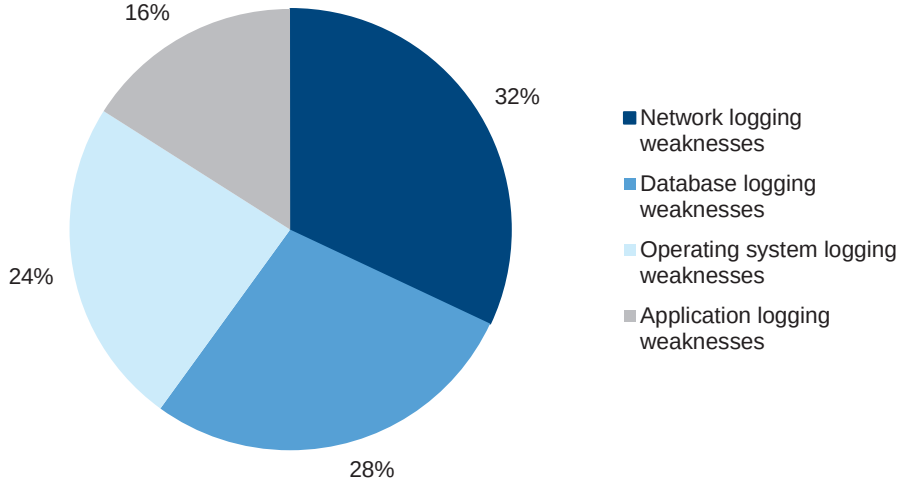
Our audit examined audit logging and monitoring of policies and procedures, as well as understanding and evaluating audit logging and monitoring controls implemented by management.

Detailed analysis of audit findings

Audit logging and monitoring of the ICT environment control weaknesses accounted for 21 audit findings, or 6 per cent, of all identified findings. There were no high-risk audit findings, with most findings rated as medium risk.

As shown in Figure 2I, the audit findings are fairly evenly distributed across the different technology layers, with a slight bias towards network logging.

Figure 2I
Audit logging and monitoring audit findings



Source: Victorian Auditor-General's Office.

Excerpts of audit findings

Figure 2J gives examples of de-identified observations noted during ICT audits as part of the 2013–14 financial audits.

Figure 2J
Typical audit logging and monitoring audit findings

- *Network monitoring at <Organisation> is administered through freeware utilities which provide limited oversight across the technical environment. These solutions are not subject to vendor support and maintenance.*
- *Audit logging has not been enabled within the <in-scope system> database.*

Source: Victorian Auditor-General's Office.

2.3.4 ICT change management

Description of the ICT general controls category

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

Why is this important?

Weaknesses in ICT change management may lead to an increased risk that unauthorised changes could be made to systems and programs. This could impact the integrity of the data of underlying financial systems.

Audit procedures performed

Our audit procedures include examining the policies and procedures governing ICT change management. Where appropriate, we performed sample testing of changes to in-scope ICT applications to validate whether the changes were appropriately authorised and tested, and whether the migration to the production environment was approved.

Detailed analysis of audit findings

ICT change management control weaknesses accounted for 28 audit findings, or 8 per cent, of the total identified findings.

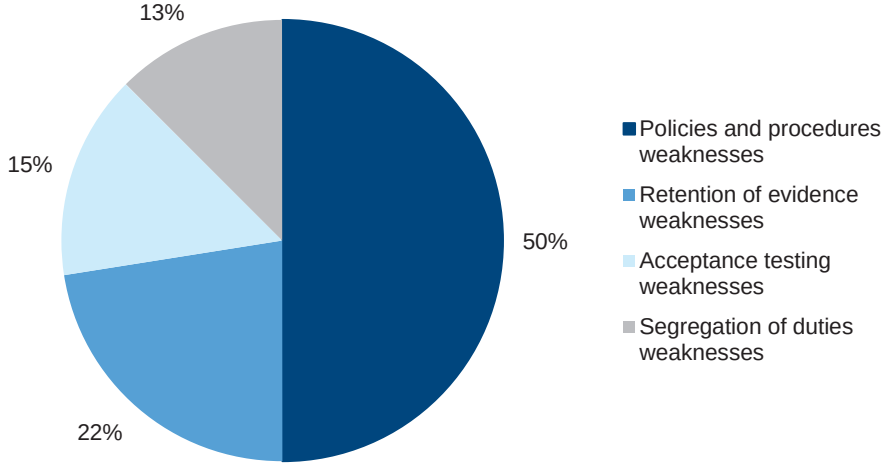
As shown in Figure 2K, there is a higher distribution of audit findings relating to policies and procedures. However, analysis of the underlying audit findings does not indicate that frameworks surrounding change management are as weak as the results suggest. This is largely due to shared findings between shared ICT environments for key financial systems.

Findings in ICT change management typically relate to:

- retention of evidence surrounding key change management controls
- absence of appropriate testing
- inappropriate segregation of duties between production and non-production environments.

As a percentage, there are relatively fewer high-risk ICT change management audit findings compared with other ICT general controls categories.

Figure 2K
ICT change management audit findings



Source: Victorian Auditor-General's Office.

Excerpts of audit findings

Figure 2L gives examples of de-identified observations noted during ICT audits as part of 2013–14 financial audits.

Figure 2L
Typical ICT change management audit findings

- Policy is silent on baseline sign-offs, documentation—such as change implementation plan—or levels of testing that must be performed before a change is implemented.
- Evidence of acceptance testing was not available at the time of the audit for five changes released into production.
- The environment which hosts < in-scope system> is also used for testing and development operations.

Source: Victorian Auditor-General's Office.

2.3.5 Patch management

Description of the ICT general controls category

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 ICT infrastructure.

Why is this important?

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

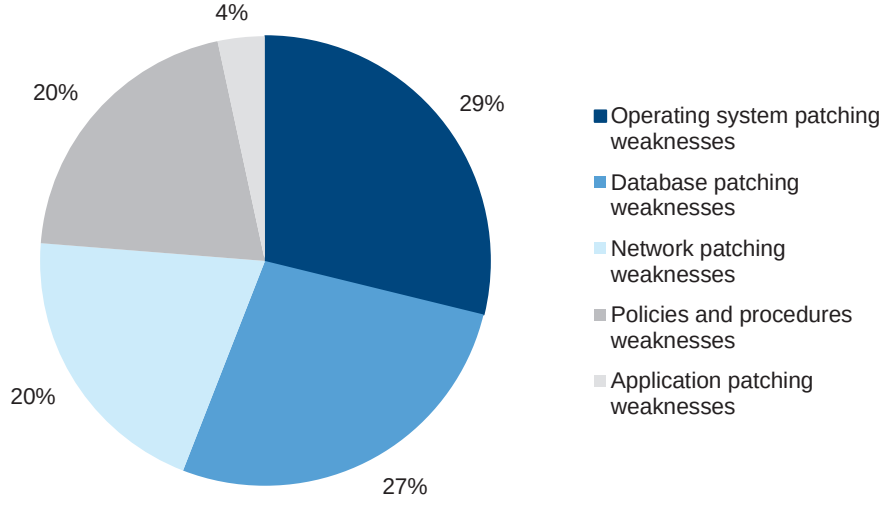
Audit procedures performed

Our audit program examines policies and procedures over patch management processes, and validates that the production environment for in-scope ICT applications has been patched by management in accordance with policies and recommended industry practices.

Detailed analysis of audit findings

Patch management control weaknesses accounted for 26 audit findings, or 7 per cent, of the total identified findings. Weaknesses in patch management controls represent 10 per cent of high-risk audit findings.

Figure 2M
Patch management audit findings



Source: Victorian Auditor-General's Office.

Patch management is a pervasive issue, impacting the majority—56 per cent—of the audited departments and agencies.

The maturity of patch management practices is variable across government. It can range from patches being omitted as a result of accidental oversight in better managed organisations, to organisations where patching is not actively managed and systems go unpatched for years.

Excerpts of audit findings

Figure 2N gives examples of de-identified observations noted during ICT audits as part of 2013–14 financial audits.

Figure 2N
Typical patch management audit findings

- The <in-scope system> has not been patched since July 2010. The current vendor-recommended patch level is dated October 2012.
- The software manufacturer released updates containing security fixes that have not been applied to the <in-scope system>.
- 21 vendor-recommended patches have not been applied to the <in-scope system> database server—i.e. the server which hosts <in-scope system> and its data. Of these, three were classed as 'critical' with the earliest patch having been made available in March 2008.

Source: Victorian Auditor-General's Office.

2.3.6 Backup management, business continuity and ICT disaster recovery planning

Description of the ICT general controls category

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

A business continuity plan (BCP) details the response strategy and process of an organisation in order to continue operations and minimise the impact in the event of a disaster.

A disaster recovery plan (DRP) is a documented process, or set of procedures, to assist in the recovery of an organisation's ICT infrastructure in the event of a disaster.

Why is this important?

Weaknesses in backup management, business continuity and ICT 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

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

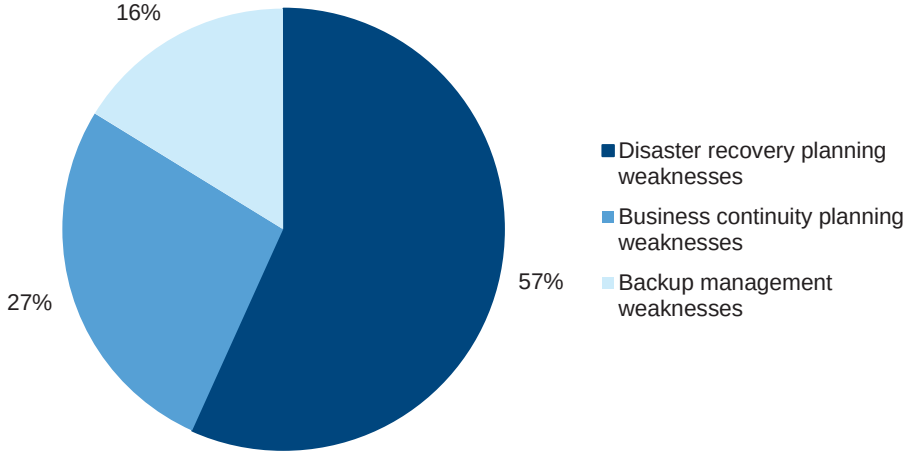
- examining whether backups are performed as intended, and whether data is periodically tested and recoverable
- examining if business continuity and disaster recovery plans exist, are updated, and are periodically tested by management.

Detailed analysis of audit findings

Collectively, backup management, business continuity and ICT disaster recovery planning accounted for 30 audit findings, or 8 per cent, of the total number of findings identified.

As highlighted in Figure 2O, the audit findings relating to disaster recovery planning require the most improvement. Findings typically range from a DRP not being updated periodically and not tested, to an absence of a formalised DRP.

Figure 2O
Backup management, business continuity and ICT disaster recovery audit findings



Source: Victorian Auditor-General's Office.

Excerpts of audit findings

Figure 2P gives examples of de-identified observations noted during ICT audits as part of 2013–14 financial audits.

Figure 2P
Typical backup management, business continuity and ICT disaster recovery audit findings

- The organisation-wide BCP is in draft. Further, a DRP for <in-scope system> has not been established. While a draft DRP is in place within the organisation, this document does not include specific guidance to support <in-scope system's> recovery in the event of a disaster.
- The disaster recovery documentation for this system has not been reviewed since November 2011. It is understood that there have been changes to system functionality and to key technical support personnel over this period to date.
- The BCP is not tested on a periodic basis.

Source: Victorian Auditor-General's Office.

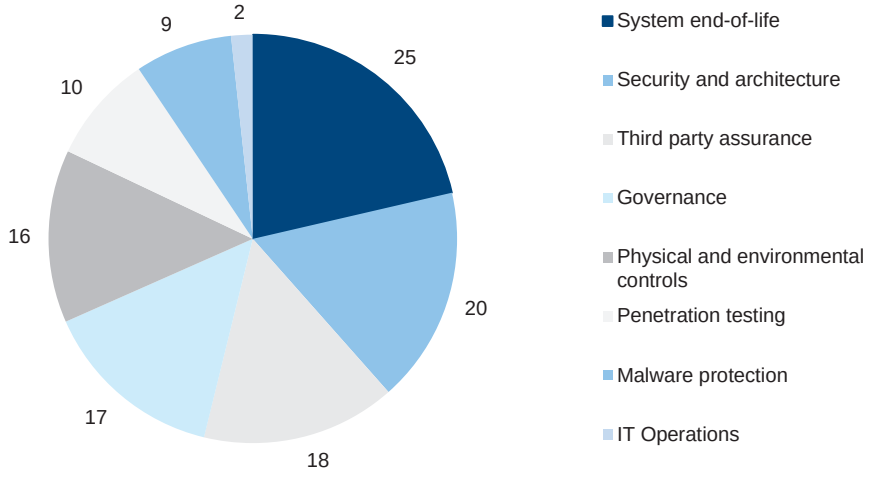
2.3.7 'Other' ICT general controls

Description of the ICT general controls category

The remaining ICT audit findings have been classified as 'other' and relate to observations that fall outside of the definition of the previous categories. These observations include:

- **Third party assurance**—relates to the assurance that third party service providers design and operate appropriate ICT controls over outsourced financial systems.
- **System end-of-life**—relates to the ICT system vendor intending to stop or limit support for its product in the near future. In some cases, vendor support has expired.
- **Security and architecture**—relates to vulnerabilities or limitations in the organisation's network security configuration or management framework.
- **Physical and environmental controls**—relates to controls surrounding in-scope applications within the data centres. Specifically, physical access to the ICT infrastructure and environment controls—such as appropriate temperature and humidity controls, and continuity of power supply.
- **Penetration testing**—relates to the process and outcomes of a technical evaluation of the internal and external vulnerabilities of ICT systems.
- **Malware protection**—relates to protection of network and computer systems from malicious software designed to cause disruption or damage to systems.
- **ICT operations**—relates to procedures and processes that support and maintain computer systems to ensure that they remain operational.
- **Governance**—relates to entity level controls including overarching frameworks, policies and standards.

Figure 2Q
'Other' ICT general controls audit findings



Source: Victorian Auditor-General's Office.

Collectively, 'other' control weaknesses accounted for 117 audit findings, or 32 per cent of the total number of findings, as well as the highest number—39 per cent—of high-risk audit findings.

About 75 per cent of the high-risk findings identified in the 'other' category relate to:

- **System end-of-life**—posing a risk to the ICT environment as a whole. Most system end-of-life audit findings tend to be rated high unless management was able to demonstrate upgrade plans or were in advanced stages of remediation prior to end of support.
- **Third party assurance**—relating to how management obtains assurance over an outsourced function or ICT environment. This is discussed in greater detail in Part 3.

Excerpts of audit findings

Figure 2R gives examples of de-identified observations noted during ICT audits as part of 2013–14 financial audits.

Figure 2R
Typical 'other' audit findings

- An Information Systems strategy has been established for the period 2013–2018. However, supporting policies, procedures and standards have not been established within the organisation.
- No technical support or system documentation is available for the interface environment.

Source: Victorian Auditor-General's Office.

2.4 ICT controls maturity assessment

One of the objectives of this report is to leverage the results of our ICT audits to assess the capability maturity of entities.

Maturity models allow an assessment of how well developed and capable the established ICT general controls are, and measure this against an objective baseline.

Initial maturity assessment

This audit used data obtained during VAGO's 2013–14 financial audits. To rate and assess the maturity of ICT controls at the audited entities we utilised definitions from a generic capability maturity model in applying the ratings.

For the 2014–15 financial year onwards, VAGO will use the *COBIT 5 Process Maturity Model*, which is based on the internationally recognised *ISO/IEC 15504 Information Technology—Process Assessment Standard.* The COBIT 5 model will require our existing audit programs to be enhanced and the compilation of additional data. This future approach will also incorporate a discussion with management on maturity scores during the ICT component of the annual financial audit.

How did we assess maturity?

Through an analysis of our ICT audit findings for the 2013–14 financial year, each entity was assessed for the maturity of its ICT general controls by category and provided with a rating. The sector maturity assessment is derived from each entity's ratings after applying simple averages.

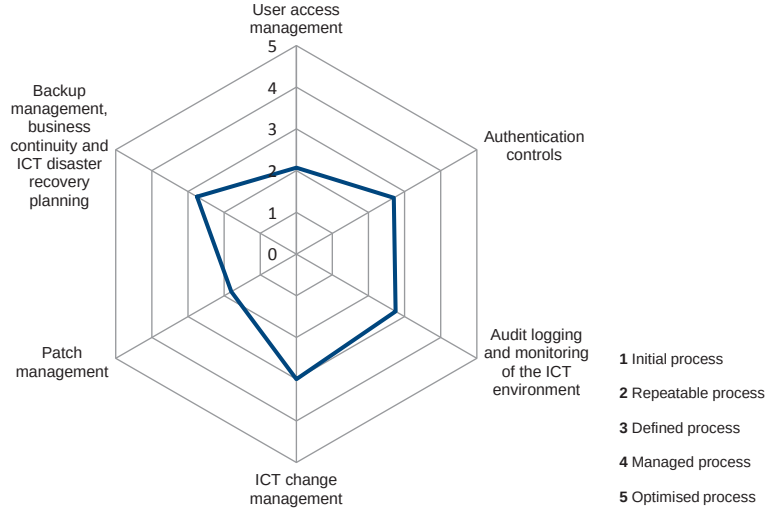
The maturity level definition is outlined below, with the five levels of capability as follows:

1. **Initial process**—no sustainable, repeatable capabilities, dependent on individual effort. No strategic view or policies to guide practices. Policies or procedures, where defined, are either ineffective, not being followed or not performed. An absence of standardised process.
2. **Repeatable process**—sustainable and repeatable practices and procedures. Some key policies may be defined to achieve a baseline level of control, but may be ineffective or out-of-date. Policies and procedures may be ill-defined but staff are aware of role and requirements. Controls across ICT environment may be inconsistent.
3. **Defined process**—defined processes to achieve a baseline level of control, practices uniformly applied. Key policies are defined but good process controls, used throughout the company, are not pervasive or vigorously enforced.
4. **Managed process**—integrated across the organisation, is governed and risk managed. Up-to-date and effective strategy, policies and procedures. Best end-to-end practice in place, standardised and enforced. Strong visibility and monitoring.

5. **Optimised process**—defined processes are embedded or continually improving. Outstanding processes are fully aligned with strategies, policies and procedures. Continuous monitoring drives process improvements. Leading processes are integrated and standardised company-wide. Proactive and complete risk management and performance.

Based on our findings for the selected 39 entities, our maturity assessment scores of the ICT general controls categories are in Figure 2S.

Figure 2S
Overall ICT maturity assessment for audited entities



Source: Victorian Auditor-General's Office.

As shown in Figure 2S, the least mature IT general controls category is patch management. Patch management had an overall average maturity score of approximately 1.8, which is between 'initial process' and 'repeatable process'.

This indicates there are a large number of entities where there is no sustainable or repeatable capability, or where policies or procedures were defined, they are either ineffective, not being followed or not performed. Although there were entities that scored 2 and more, the average score is relatively low.

The results of our ICT audits suggest ICT change management is a more mature ICT general controls category. In a number of entities we audited, there are defined ICT change policies and procedures guiding the overall process, and key governance structures within the organisation are involved in ensuring that duly authorised, approved and tested changes are implemented into the live ICT environment.

Conclusion

Consistent with our overview and themes, our capability maturity assessment for financial year 2013–14 assessments highlights the need for entities to urgently establish better controls to manage:

- user access management
- patch management.

3 Themes from ICT audits

At a glance

Background

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

Conclusion

For the 2013–14 financial year, we identified five clear emerging themes from ICT audits, with a number of recommendations that can be put in place to address them.

Findings

The five themes identified through our ICT audits are:

- ICT security controls need improvement
- management of service organisation assurance activities requires attention
- prior-period audit findings are not being addressed in a timely manner
- patch management processes need improvement
- ICT disaster recovery planning is weak.

Recommendations

Noting the high-level findings, public sector entities—governing bodies and management—and DSDBI, should:

- enforce ICT security policies and procedures, including improving user access management, authentication controls and patch management processes
- develop and implement appropriate policy and guidance on assurance activities surrounding outsourced ICT arrangements
- enhance their understanding of the Assurance or Auditing Standards requirements for service assurance reports
- implement actions to address control weaknesses in outsourced ICT arrangements
- implement sustainable process improvements to prevent re-occurring audit findings
- through audit committees, implement appropriate monitoring mechanisms to ensure audit findings are addressed by management
- develop appropriate ICT disaster recovery capabilities, involving ICT service providers as necessary.

3.1 Introduction

This Part provides insight on:

- the top five themes noted during the information and communications technology (ICT) audits conducted for the 2013–14 financial year
- root cause analysis and insights into the ICT audit themes
- strategic implications and recommendations for possible future action plans.

3.2 Top five themes noted in 2013–14

Based on our analysis of the ICT audit issues noted during 2013–14, the top five themes were:

- ICT security controls need improvement
- management of service organisation assurance activities require attention
- prior-period audit findings are not being addressed in a timely manner
- patch management processes need improvement
- ICT disaster recovery planning is weak.

3.2.1 ICT security controls need improvement

Our observations

ICT security audit findings are within the following ICT general controls categories:

- user access management
- authentication controls
- patch management
- audit logging and monitoring of ICT environment
- other ICT general control sub-categories, including malware protection, penetration testing, physical and environment controls, security and architecture.

Collectively, the audit findings from the above ICT general controls categories account for 67 per cent of all audit findings reported in the 2013–14 financial year. These ICT security audit findings affected 36 of the 39 entities in-scope for this report.

When analysed by risk rating, 38 of the 69 high-risk findings (55 per cent) relate to ICT security weaknesses, highlighting the need for public sector chief information officers (CIO) to focus additional effort on ICT security processes and controls.

Insights and implications

Our analysis of these findings identified the following probable causes:

- **Lack of enforcement**—as noted from the detailed analysis in Part 2, the 2013–14 financial audits show that about 65 per cent of our audit findings are due to laxity or lack of enforcement by management.
- **Lack of monitoring controls**—there is an opportunity for management to implement controls that periodically monitor the ICT environment and its security. Monitoring controls could include process health checks to make sure that controls are functioning as designed, and if there are lapses, that they are detected and corrected on a timely basis.

Given the frequency of these audit findings and its associated risk rating, it is vital that management focus on ICT security processes and controls, and increase enforcement of the organisation's ICT security policies.

3.2.2 Management of service organisation assurance activities require attention

Our observations

When a department or public sector agency relies on an outsourced provider to operate and maintain ICT controls, they need to obtain assurance that the controls managed by the outsourced provider have been operating effectively during the financial year. Assurance over effectiveness of the control environment at outsourced service providers is part of the overall internal control framework of an entity. By using an outsourced ICT arrangement, the entity's management does not forego its duty to ensure that controls are adequate and that sensitive data and information is protected.

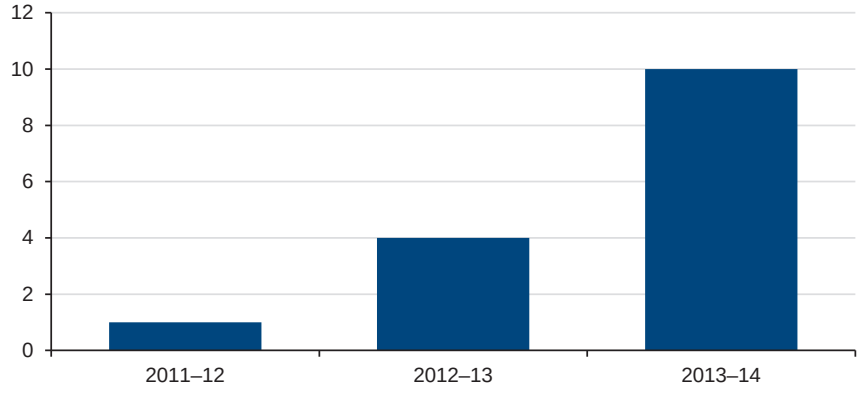
In the context of the Victorian public sector, the service organisation is the provider of the ICT services, such as CenITex and private providers. The user entity is the department or public sector agency, and their auditor is VAGO.

The Australian Standard on Assurance Engagements, ASAE 3402 *Assurance Reports on Controls at a Service Organisation,* outlines the requirements for assurance practitioners who are engaged to provide an assurance report on the controls at a service organisation for user entities and their auditors. Although ASAE 3402 reports are typical of what we receive, there are also other reports provided under other standards, such as Auditing Standard AUS810 *Special purpose reports on the effectiveness of control procedures*, which account for 10 per cent of the service assurance reports we received.

There is a noticeable upward trend in the number of service assurance reports and similar instruments obtained by public sector entities, which they relied upon for financial reporting purposes and VAGO utilised as part of our financial audits.

In the 2013–14 financial year, there were 10 service assurance reports shared with VAGO for the ICT general controls operating at outsourced ICT environments. This compares to four reports received for the 2012–13 financial year and one for the 2011–12 financial year. This trend is shown in Figure 3A.

Figure 3A
Number of service assurance reports received



Note: Where a service assurance report is prepared over a shared ICT environment such as CenITex, these are accounted for in the graph as one report.
Source: Victorian Auditor-General's Office.

Given that two of the government's goals are to outsource the CenITex-based ICT infrastructure and for entities to consider using cloud-based applications, it is likely that reliance by management and VAGO on such reports will continue. Of the 10 service assurance reports that were obtained by entities in 2013–14, there was one report that, in our opinion, did not comply with the requirements of the assurance standards. VAGO reported this as a high-risk issue in our management letters to the affected entities.

When analysed by risk rating, 11 of the 69 high-risk findings identified during the 2013–14 financial year (16 per cent) related to service assurance reports. These findings were due to an absence of assurance, or the prepared report not complying with the requirements of the assurance standard.

Insights and implications

Outsourcing to the private sector and the growth of cloud-based ICT services is likely to impact on the public sector and VAGO as follows:

- **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. How an agency chooses to do so may require further policy guidance, as our findings show that a number of agencies do not currently obtain any form of assurance over controls operating at outsourced service providers.

- **Prevalence and maturity**—given the government's outsourcing goals, there will likely be an increase in the assurance being sought through service assurance reports. It is important that each entity's management has more awareness of such instruments, particularly about what the Assurance or Auditing Standards require and how management is able to leverage such reports to achieve their *Financial Management Act 1994* obligations and operate an effective and secure internal controls framework.
- **Accountability**—as the control environment may not be directly under management's control, there may be a perception that risks and audit findings have been outsourced, which is not the case. Under the provisions of the *Financial Management Act 1994* and the Standing Directions of the Minister for Finance, the public sector entity's accountable officer is ultimately responsible for maintaining an effective internal control environment over its transactions.
- **Enhanced reporting to audit committees**—with potentially more ICT applications being audited under such arrangements in future years, ICT general controls testing performed directly by VAGO may reduce, as more audit findings may be noted within service assurance reports. The potential reduction in audit findings within VAGO management letters may lead some entities to believe that the overall ICT controls environment is improving. To mitigate this risk, from the 2014–15 financial year onwards, we will summarise relevant audit findings highlighted by the service auditor in our management letters and also check whether management activities to address the control weaknesses are documented.

3.2.3 Prior-period audit findings are not being addressed in a timely manner

Our observations

A number of the ICT general controls weaknesses raised in prior years have not been addressed by entities, despite agreement and commitment by management to resolve them.

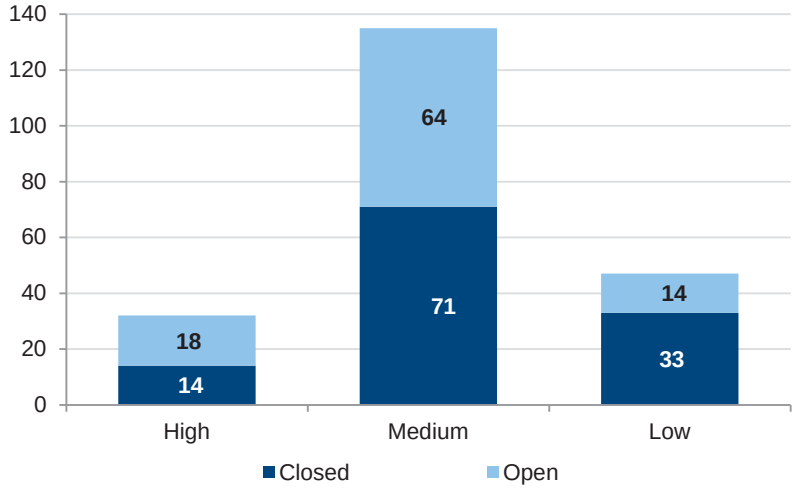
Of the 214 ICT audit findings included in prior-year management letters, 118 (55 per cent) were addressed by management. The remaining 96 findings were re-raised in the 2013–14 financial year management letters, as they were either not fully addressed, or activities did not ensure that further control weaknesses would not re-occur.

Of the 96 prior period open issues identified:

- 19 per cent were high-risk audit findings
- 67 per cent were medium-risk audit findings
- 15 per cent were low-risk audit findings.

As shown in Figure 3B, management is having relatively better success at addressing low-risk issues, but is failing to adequately address higher-risk control weaknesses.

Figure 3B
Prior-period audit findings by rating



Source: Victorian Auditor-General's Office.

Insights and implications

Based on our discussions with management, and supplemented by a high-level analysis of our data, our insights relating to prior-period audit findings are as follows:

- **Fixing symptoms rather than implementing process improvements**—although management is generally efficient at addressing audit findings that have been reported by the auditors, they are less effective in implementing process improvements. An example of a symptom might be 'inappropriate access granted to users'—once reported, management would remove the access without necessarily implementing periodic user access reviews or improving existing user access provisioning or removal processes, which is required to ensure the audit finding does not re-occur.
- **High-risk system end-of-life audit findings**—nine of the 18 high-risk prior-period open audit findings are associated with system end-of-life for the use of software such as Microsoft Windows 2000, Windows XP and applications that have limited vendor support. Technology refresh projects typically require a longer period for entity management to action as the ICT project life cycle generally involves budget funding and allocation processes, business cases and approval gates, as well as time to deliver outcomes. We will continue to review key financial ICT infrastructure for system end-of-life risk and monitor management's plans and report as necessary.
- **Period of time taken to complete management actions**—a number of ICT audit findings from prior years have remained un-addressed for an extended period of time.

- **Role of the audit committee**—as a key governance body, there is an expectation that the audit committee would hold the entity's management responsible for un-actioned audit findings. Given the large number of prior-year audit findings that are not being addressed, it is important that the audit committees set the appropriate tone at the top and oversee appropriate management action.

While some findings, such as high-risk system end-of-life audit findings, require more time to address, these findings account for a relatively small proportion of our overall prior-period issues. Re-occurring audit findings are likely a reflection of management's attitude towards maintaining a well-managed ICT environment and functional controls and the general lack of resources or funding.

A poorly managed ICT control environment poses a higher risk of controls being bypassed and a higher risk to the integrity of underlying financial data that supports the financial reporting process.

3.2.4 Patch management processes lacks maturity

Our observations

A patch is an additional piece of software designed to fix security vulnerabilities or operational issues.

The Australian Signals Directorate (ASD) is the Australian Government's key information security agency, and provides advice and assistance on information and communication security to all Australian government jurisdictions. According to the ASD, at least 85 per cent of targeted cyber intrusions can be mitigated by implementing ASD's '*Top 4 Strategies to Mitigate Targeted Cyber Intrusions'.*

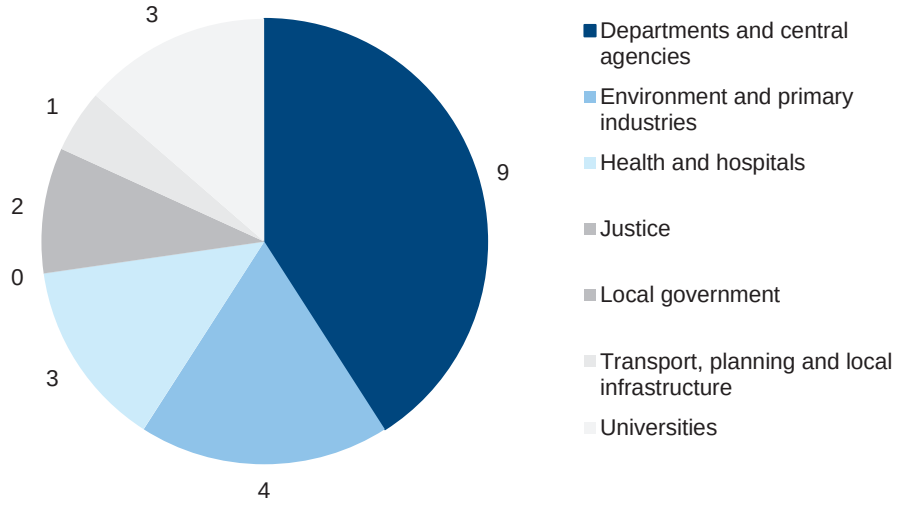
The Victorian Government's information security standards require 'inner whole-of-Victorian-Government (WoVG) agencies' to implement ASD's top four strategies. Two of these strategies relate to patching, specifically:

- maintain up-to-date software patches for applications
- maintain up-to-date patches of operating systems.

The scope of this report covers 14 of the 20 inner WoVG agencies. Inner agencies include government departments, Victoria Police, Public Transport Victoria, Ambulance Victoria, CenITex, Country Fire Authority, VicRoads, the Environment Protection Authority Victoria, the Victoria State Emergency Service and the Emergency Services Telecommunications Authority.

Figure 3C shows how these findings are distributed across the departments and agencies in scope, with all government sub-sectors equally represented. Of the 39 selected departments and agencies, 22 (or 56 per cent) had open audit findings relating to patch management.

Figure 3C
Entities with patch management related issues



Source: Victorian Auditor-General's Office.

Although this does not directly suggest a strong trend of patch management related weaknesses, it is important to note that where patch management issues are reported, there is a greater probability that the audit finding is higher risk, with patch management high-risk issues accounting for 10 per cent of the high-risk findings reported in the 2013–14 financial year.

Of the ICT general controls categories discussed in this report, patch management is ranked the lowest in terms of process maturity.

Our observations are consistent with VAGO's *WoVG Information Security Management Framework* performance audit report, tabled in November 2013, which identified patching issues at all examined entities. The performance audit report also noted that the biggest impediment to patching was a lack of resources to test the impact of vendor patches on entity networks and software applications.

Other probable causes for patch management findings have been articulated earlier in this Part, and they relate to:

- lack of enforcement
- lack of monitoring controls
- fixing symptoms and not implementing process improvements.

3.2.5 ICT disaster recovery planning is weak

Our observations

An ICT disaster recovery plan (DRP) is a documented process, or set of procedures, to assist in the recovery of an organisation's ICT infrastructure in the event of a disaster. In the 2013–14 financial year, there are 21 findings related to DRP, five of which are high-risk rated audit findings, which account for 7 per cent of all reported high-risk findings.

The analysis of these audit findings shows that they are spread across government, suggesting a general need for greater effectiveness in the way public sector entities manage and restore ICT services after a significant event—such as a large scale disaster. Although these are reported to each entity's management, there are broader issues underlying ICT disaster recovery as a capability within government that require urgent attention.

One of the findings relating to disaster recovery planning is related to a key provider of ICT services to government which does not have a formalised ICT disaster recovery plan. There is also no framework surrounding how this service provider prioritises and responds to a significant event—such as a disaster impacting a number of supported departments and agencies—which would place unprecedented strain on its manpower and resource pool.

This observation is consistent with VAGO's *Portfolio Departments and Associated Entities: Results of the 2012–13 Audits,* which found that:

- the service provider does not have sufficient ICT disaster recovery capability to respond to a significant event
- departments and agencies are not informing themselves adequately about the service provider's ICT disaster recovery capability
- because it is unassessed and unmanaged, the risk of ICT failure after a significant event is significant and unacceptable
- although the service provider had advised the departments and agencies in its annual attestations that it does not having an ICT disaster recovery plan to address significant failures, there had been no action by the service provider to address the risk.

As the role of this service provider changes in the future, the affected departments and agencies will need to ensure this risk is tracked and sufficiently managed to safeguard the continuity of its operations and delivery of services to the public. It is critical that government assess, invest and develop an appropriate ICT disaster recovery framework at a WoVG-level.

Recommendations

Noting the high-level findings, public sector entities—governing bodies and management—and the Department of State Development, Business and Innovation, should:

1. enforce information and communication technology security policies and procedures, including improving user access management, authentication controls and patch management processes
2. develop and implement appropriate policy and guidance on assurance activities surrounding outsourced information and communication technology arrangements
3. enhance their understanding of the Assurance or Auditing Standards requirements for service assurance reports, ensure that reports received are fit for purpose and provide an accurate reflection of the control environment
4. implement actions to address control weaknesses in outsourced information and communication technology arrangements.
5. implement sustainable process improvements to prevent re-occurring audit findings.
6. through audit committees, implement appropriate monitoring mechanisms to ensure audit findings are addressed by management
7. develop appropriate information and communication technology disaster recovery capabilities, involving information and communication technology service providers as necessary.

Appendix A.
Rating definitions

Ratings for audit issues 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 or • a **material** misstatement in the financial report has occurred.	Requires immediate management intervention with a detailed action plan to be implemented within one month. 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 or • a **material** misstatement in the financial report that is likely to occur.	Requires prompt management intervention with a detailed action plan implemented within two months. Requires executive management to correct the material misstatement in the financial report to avoid a modified audit opinion.
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.

Figure A1
Rating definitions and management action – *continued*

Rating	Definition	Management action required
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.

ICT controls report 2013–14: scope and coverage

Figure B1
Selected entities that are in scope for ICT controls report 2013–14

Entities	Sector
Department of Education and Early Childhood Development	Department and central agencies
Department of Environment and Primary Industries	Department and central agencies
Department of Health—includes health and shared services	Department and central agencies
Department of Human Services	Department and central agencies
Department of Justice	Department and central agencies
Department of Premier and Cabinet	Department and central agencies
Department of State Development, Business and Innovation—includes CenITex	Department and central agencies
Department of Transport, Planning and Local Infrastructure	Department and central agencies
Department of Treasury and Finance—includes State Revenue Office	Department and central agencies
State Trustees Limited	Department and central agencies
Victoria Police	Department and central agencies
Central Gippsland Regional Water Corporation	Environment and primary industries
City West Water Corporation	Environment and primary industries
Coliban Region Water Corporation	Environment and primary industries
Goulburn-Murray Region Water Corporation	Environment and primary industries
Melbourne Water Corporation	Environment and primary industries
South East Water Corporation	Environment and primary industries
Vicforests	Environment and primary industries
Yarra Valley Water Corporation	Environment and primary industries
Austin Health	Health and hospitals
Australian Health Practitioner Regulation Agency	Health and hospitals
Ambulance Victoria	Health and hospitals
Ballarat Health Services	Health and hospitals
Barwon Health	Health and hospitals
Melbourne Health	Health and hospitals
Monash Health	Health and hospitals
Peter MacCallum Cancer Centre	Health and hospitals

Figure B1
Selected entities that are in scope for
ICT controls report 2013–14 – *continued*

Entities	Sector
The Royal Children's Hospital	Health and hospitals
The Royal Women's Hospital	Health and hospitals
Western Health	Health and hospitals
Victorian Commission of Gambling and Liquor Regulation	Justice
Greater Geelong City Council	Local government
Mornington Peninsula Shire Council	Local government
Places Victoria	Transport, planning and local infrastructure
Public Transport Victoria	Transport, planning and local infrastructure
Deakin University	Universities
Monash University	Universities
Royal Melbourne Institute of Technology	Universities
Swinburne University	Universities

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, or part of this report, was provided to the Department of State Development, Business and Innovation.

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 State Development, Business and Innovation

Department of State Development, Business and Innovation

121 Exhibition Street
Melbourne Victoria 3000
Australia
GPO Box 4509
Melbourne Victoria 3001
Australia
Telephone: (03) 9651 9999
Facsimile: (03) 9651 9770
www.dsdbi.vic.gov.au
DX210074

Mr John Doyle
Auditor - General
Victorian Auditor-General's Office
Level 24
35 Collins Street
MELBOURNE VIC 3000

Dear Mr Doyle

Thank you for your letter dated 3 October 2014: *Audit Act 1994, S16(3) - Proposed Audit Report, Information and Communication Technology Controls Report 2013-14.*

Please note that your letter, and its enclosed extracts of your proposed report, was received on 7 October 2014 and requested a formal response from me by 10 October 2014.

I note that the report summarises the results of the audits of ICT general controls as part of the annual financial audits of 39 selected entities including government departments, hospitals, local government and universities. On the basis of these audits, VAGO has prepared management letters advising these entities of any identified control weaknesses. It is my understanding that these entities, including DSDBI, have responded to these VAGO findings.

In respect of DSDBI's lead agency role for ICT, led within the Department by the Chief Technology Advocate (CTA), I provide the following comments.

The formal scope of public entities within the purview of the CTA is described in the *Victorian Government ICT Strategy* (see listing attached). This scope is smaller than the range of entities covered by the audit. This means that comments relating to action by DSDBI via the CTA can only encompass action relating to those agencies, not the larger set of agencies encompassed in the audit. I note also that the CIO Council and CFO Forum with whom your Office also consulted have a lesser scope than the agencies covered in the audit. This point is pertinent in that DSDBI is named specifically in the lead-in to the recommendations of the audit, but has no authority to influence the majority of the sectors set out in Figure 1C of the report; for example: hospitals, local government and universities.

The lead-in to the recommendations also requires public sector entities to address the recommendations, as well as DSDBI. It would be clearer if the recommendations relating only to the entities themselves were differentiated from those that included DSDBI in its lead role via the CTA.

RESPONSE provided by the Secretary, Department of State Development, Business and Innovation – continued

In relation to the specific recommendations, my comments are set out below.

Recommendation 1

The recommendation is sound. However, it is noted that the CTA's role in respect of ICT is one of advocacy and setting of policy/guidance, and that the authority to enforce policies and procedures in any agency rests with each agency's Secretary or CEO. It is therefore assumed that this recommendation is only for the entities themselves, and not the CTA. I would be grateful if this was made clearer.

Recommendations 2, 3 and 7

The recommendations are sound. It is agreed that entities would gain from undertaking this work. It is accepted that there is also a role for the CTA to issue guidance on this to the agencies within the scope of the CTA.

Recommendations 4, 5 and 6

The recommendations are sound. It is agreed that entities would gain from undertaking this work. However, there is no role for the CTA in relation to these recommendations. I would be grateful if this was made clearer.

Finally, I note that while the scope of the CTA is restricted, this has not stopped 'outer' agencies utilising the advice and guidance issued by the CTA (it is publicly available). Advice issued by the CTA as a result of audit recommendations 2, 3 and 7 may have broader use than the restrictions in scope would imply.

Thank you for the opportunity to respond.

Yours sincerely

Howard Ronaldson
SECRETARY

RESPONSE provided by the Secretary, Department of State Development, Business and Innovation – continued

Attachment

Public entities within the scope of the CTA

All Departments
Department of Education and Early Childhood Development
Department of Environment and Primary Industries
Department of Health
Department of Human Services
Department of Justice
Department of Premier and Cabinet
Department of State Development, Business and Innovation
Department of Transport, Planning and Local Infrastructure
Department of Treasury and Finance

Agencies
Ambulance Victoria
CenITex
Country Fire Authority
Emergency Services Telecommunications Authority
Environment Protection Authority
Metropolitan Fire and Emergency Services Board
Public Transport Victoria
State Revenue Office
Victoria Police
VicRoads
Victoria State Emergency Service

Auditor-General's response to the Department of State Development, Business and Innovation

I would like to thank you for the comments provided.

I acknowledge the formal scope of public entities within the Chief Technology Advocate's (CTA) mandate and your comments that 'while the scope of the CTA is restricted, this has not stopped 'outer' agencies utilising the advice and guidance by the CTA (it is publicly available)'. I believe my view is consistent with the department's understanding, in that the role of the CTA is one of strategic leadership and 'strengthening of ICT governance' within government. This includes providing leadership in the form of publicly available advice and guidance.

I confirm that each entity's management and governing body is the accountable party for completing remedial action arising from detailed audit findings reported at their respective agencies. Notwithstanding, it should be noted that 50 per cent of the analysed audit findings for *Information and Communications Technology Controls Report 2013–14* relate to departments and agencies within the purview of the CTA. Given the origins of the audit findings and how the audit findings are distributed, I am of the view that the engagement of the CTA and the department is appropriate and will positively influence remedial action.

I would also like to clarify that the letter and proposed draft report, dated 3 October 2014, was hand delivered to your nominated delegate on 2 October 2014 in a meeting at 5 00 pm. As the letter and draft report were provided after hours, professional courtesy was extended by dating the letter to the next business day. The turnaround response time requested is in accordance with other similar reports from my office and was included in the briefing with your department and nominated delegate.

Auditor-General's reports

Reports tabled during 2014–15

Report title	Date tabled
Technical and Further Education Institutes: Results of the 2013 Audits (2014–15:1)	August 2014
Coordinating Public Transport (2014–15:2)	August 2014
Managing the Environmental Impacts of Transport (2014–15:3)	August 2014
Access to Legal Aid (2014–15:4)	August 2014
Managing Landfills (2014–15:5)	September 2014
Management and Oversight of the Caulfield Racecourse Reserve (2014–15:6)	September 2014
Effectiveness of Catchment Management Authorities (2014–15:7)	September 2014
Heatwave Management: Reducing the Risk to Public Health (2014–15:8)	October 2014
Emergency Response ICT Systems (2014–15:9)	October 2014
Public Sector Performance Measurement and Reporting (2014–15:10)	October 2014
Mental Health Strategies for the Justice System (2014–15:11)	October 2014

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

Or contact us at:

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