Information and Communications Technology Controls Report 2013–14

Tabled 15 October 2014

Background

pages 1–8

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

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

Audit objectives

page 1

- Summarise the results of our audits of public sector entities' ICT general controls (2013–14).
- Provide additional insight into and more visibility of our ICT audit findings.
- Provide decision-makers with relevant information to assist them to address audit findings and improve processes.
  - Improved processes leading to increased efficiencies – benefits to agencies and the auditing function.

Context of this report

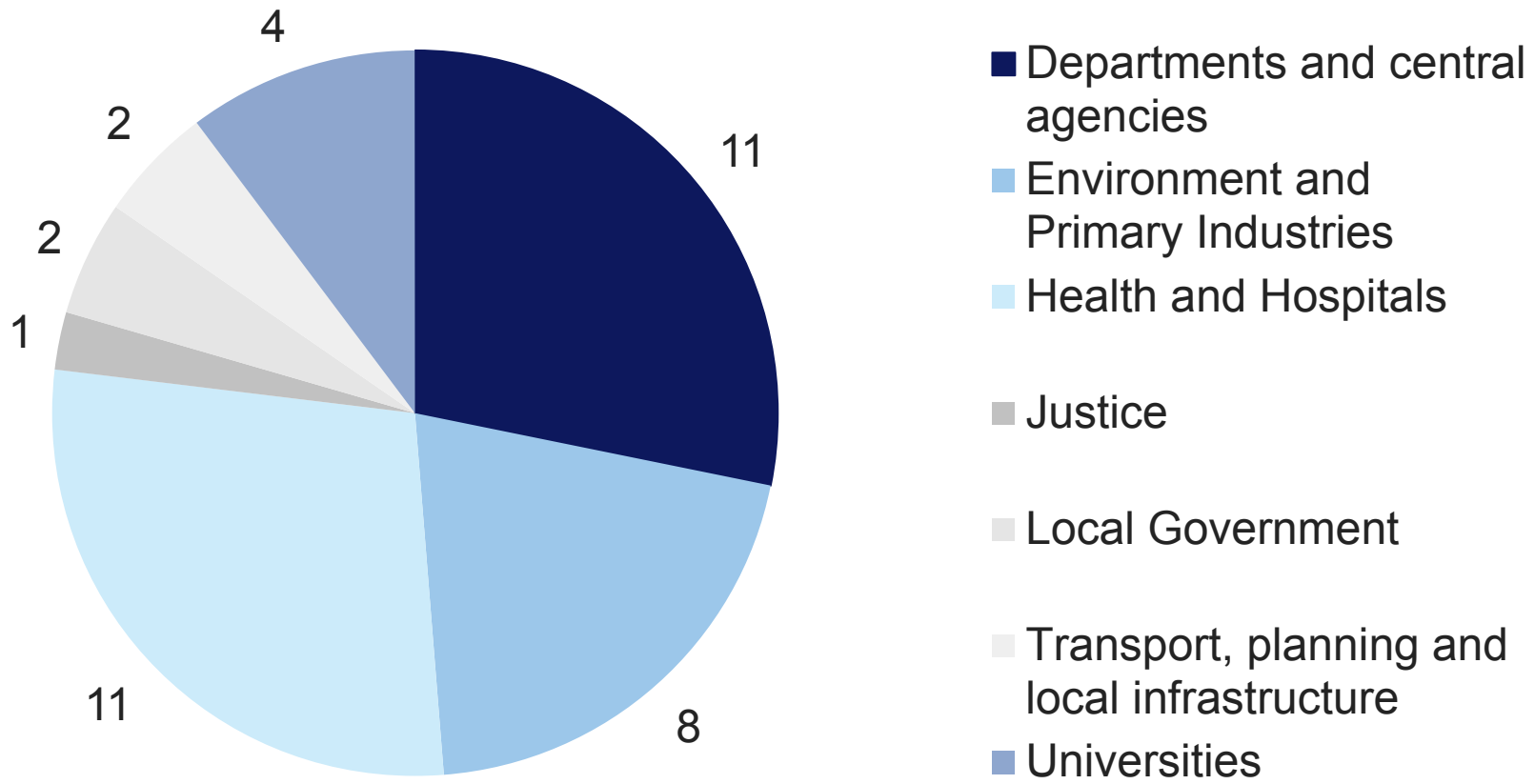
- This report is the first of its type and reflects VAGO's increased scrutiny of ICT systems.
  - It is currently limited to financial ICT systems, but we aim to expand this scrutiny to operational systems in future reports.
- This information is not usually made public, nor is it disclosed in Minister for Finance reports to the Parliament.
- VAGO has decided to report these aggregate issues in the interests of greater transparency and accountability.

Context of this report – *continued*

- All findings used for this report have been previously communicated to governance bodies and accountable officers via audit 'management letters' or via third party assurance reports.
- In the future, we will also perform detailed maturity assessments of audited entities' ICT environments and examine selected areas of focus, such as:
  - identity and access management
  - software licensing
  - wireless network security
  - general information security strategies.

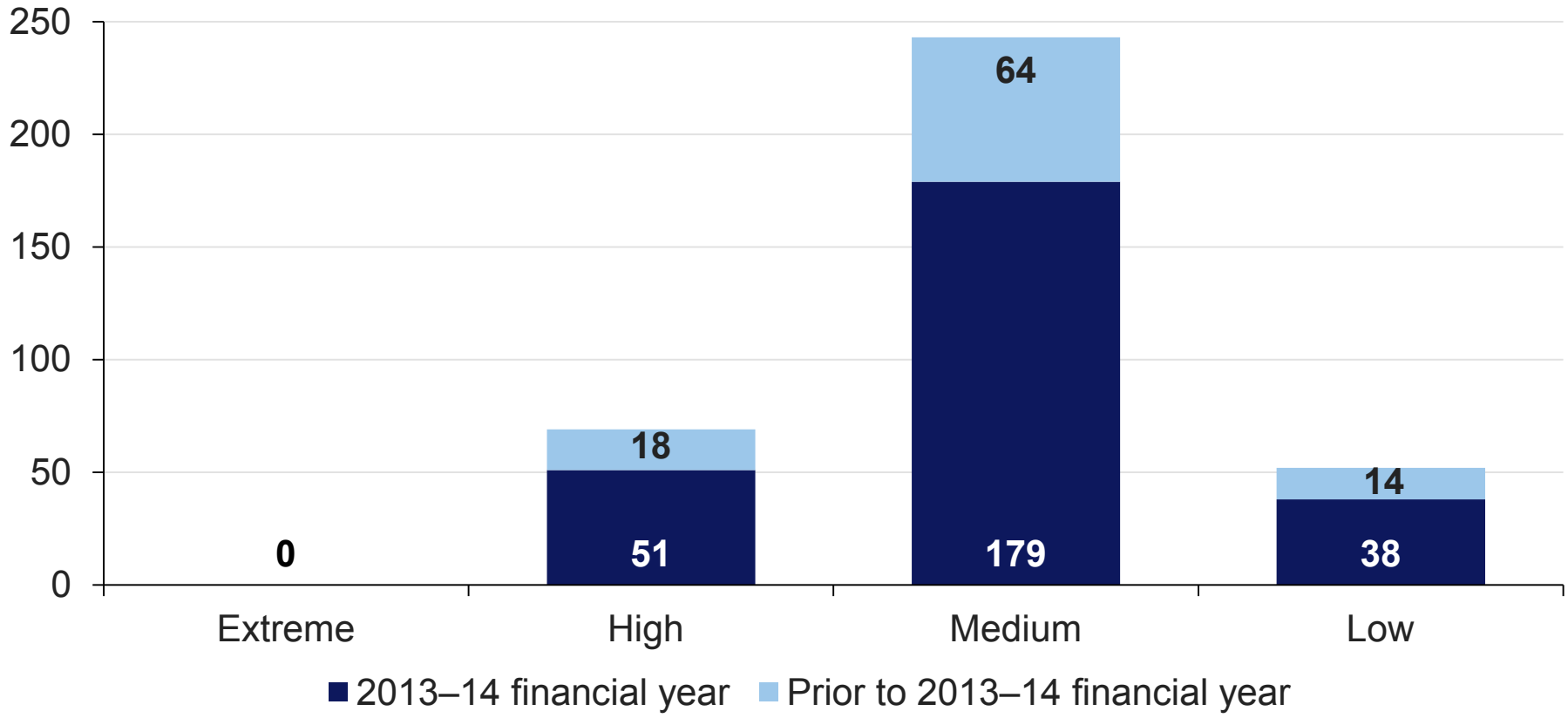
Scope and coverage

- 39 selected entities across government.



Scope and coverage – *continued*

- 64 key financial applications were audited.
- 364 ICT audit findings—open and prior year



Conclusions

- Despite some deficiencies in ICT controls, VAGO was able to rely on these controls for financial reporting purposes because other mitigating controls were identified and tested.
  - However this extra testing work by VAGO adds to costs for agencies to conduct financial audits.
- Most of the ICT audit findings were medium risk, with none rated as extreme.
- Five key themes were noted for the 2013–14 financial year.

Findings

High-risk ICT audit findings accounted for 87 per cent of all high-risk findings and were concentrated around the following ICT general controls categories:

pages 9–27

1. Managing access to ICT applications and data:
   - for example, departed employees still have log-ons.
2. Assurance obtained by entities over ICT general controls performed by external organisations:
   - for example, third party assurance reports not being obtained.
3. Entities using ICT systems that are no longer supported by vendors:
   - for example, software—application or operating system—is obsolete.

Findings – *continued*

pages 9–27

4. Authenticating users to ICT systems
   - for example, passwords are weak and easy to guess.
5. Software patch management, such as implementing software release by vendors to fix security vulnerabilities or operational issues.
   - for example, software patching taking many months or years.
6. Maintaining processes to assist in the recovery of an entity's ICT systems in the event of a disaster.
   - for example, no whole-of-government capability exists to recover the core financial systems after a catastrophic outage.

Five key themes

The five themes identified from our ICT audits were:

pages 29–38

1. ICT security controls need improvement
2. management of service organisation assurance activities requires attention
3. prior-period audit findings are not being addressed in a timely manner
   - 45 per cent outstanding and most work done on low-risk issues
4. patch management processes need improvement
5. ICT disaster recovery planning is weak.

Recommendations

		Accept
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 communications 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 communications technology arrangements.	✓
3.	enhance their understanding of the assurance or auditing standards requirements for service assurance reports.	✓

Recommendations – *continued*

		Accept
Noting the high-level findings, public sector entities—governing bodies and management—and the Department of State Development, Business and Innovation, should:		
4.	implement actions to address audit findings in outsourced information and communications technology arrangements	✓
5.	implement sustainable process improvements to prevent re-occurring findings	✓
6.	through audit committees, implement appropriate monitoring mechanisms to ensure audit findings are addressed by management	✓
7.	develop appropriate information and communications technology disaster recovery capabilities, involving ICT service providers as necessary.	✓

Contact details

For further information on this presentation please contact:

Victorian Auditor-General's Office
[p] 8601 7000
[w] www.audit.vic.gov.au/about_us/contact_us.aspx