Appendix C:
Audit scope and method

Scope of this audit

Who we examined

We examined the following agencies. The report does not identify the agencies in detail due to potential security risks.

Agency	Their key responsibilities
Cenitex	Cenitex is a state-owned enterprise that delivers ICT services to Victorian Government departments and agencies.
• Department of Education • Department of Energy, Environment and Climate Action • Department of Families, Fairness and Housing • Department of Government Services • Department of Health • Department of Jobs, Skills, Industry and Regions • Department of Justice and Community Safety • Department of Premier and Cabinet • Department of Transport and Planning • Department of Treasury and Finance	Agencies are accountable for the cybersecurity of their servers and are responsible for establishing, implementing and maintaining technical security controls for all their servers. This includes ensuring technical security controls are effective, including for those on servers managed by third parties.

Our audit objective

Do agencies' cybersecurity measures protect their IT servers from threats?

What we examined

We examined if agencies:

- track their inventory of physical and virtual servers
- have technical security controls in place for their servers that:
  - align with foundational benchmark technical security controls
  - work as intended
- monitor, report and act to improve their server security.

We did not examine:

- cybersecurity in department portfolio entities
- servers that agencies use to support operational technology, such as traffic lights
- the effectiveness of threat and vulnerability monitoring and reporting tools.

Aspects of performance examined

Our mandate for performance audits and reviews includes the assessment of economy, effectiveness, efficiency and compliance (often referred to as the '3Es + C').

In this audit we focused on the following aspects:

Economy	Effectiveness	Efficiency	Compliance
○	●	○	○

Key:

- ● Primary focus
- ◐ Secondary focus
- ○ Not assessed

Conducting this audit

Assessing performance

To form a conclusion against our objective we used the following lines of inquiry and associated evaluation criteria.

Line of inquiry		Criteria	
1.	Do agencies track all their servers and apply foundational security controls to them?	1.1	Agencies have a complete and accurate server inventory.
		1.2	Agencies apply technical security controls to their servers that align with foundational controls in relevant global benchmarks.
2.	Do agencies monitor their server security and strengthen it in response to threats?	2.1	Agencies monitor and report on server threats, vulnerabilities and whether their security controls work as intended.
		2.2	Agencies use their monitoring information to improve their server security controls and reduce vulnerabilities.

Our methods

As part of the audit, we:

- assessed:
  - 10 government departments' and Cenitex's server inventory
  - how agencies configure their technical security controls on their servers
  - if agencies monitor their server security and use this monitoring to strengthen it
- interviewed key staff
- contracted subject-matter experts to:
  - assess server inventory information provided by agencies
  - develop a survey with technical security controls in line with relevant standards and frameworks
  - analyse how agencies have configured their technical security controls
  - provide findings based on this analysis.

Level of assurance

In an assurance review, we primarily rely on the agency's representations and internally generated information to form our conclusions. By contrast, in a performance audit, we typically gather evidence from an array of internal and external sources, which we analyse and substantiate using various methods. Therefore, an assurance review obtains a lower level of assurance than a performance audit (meaning we have slightly less confidence in the accuracy of our conclusion).

Compliance

We conducted our audit in accordance with the *Audit Act 1994* and ASAE 3500 Performance Engagements to obtain reasonable assurance to provide a basis for our conclusion.

We complied with the independence and other relevant ethical requirements related to assurance engagements.

Cost and time

The full cost of the audit and preparation of this report was $791,000.

The duration of the audit was 11 months from initiation to tabling.