Appendix C:
Audit scope and method

Scope of this audit

Who we examined

There are 10 agencies included in the audit scope:

- Cenitex (we did not examine its internal cybersecurity controls but its management of the shared Microsoft 365 tenancy)
- Department of Education (renamed from Department of Education and Training on 1 January 2023)
- Department of Government Services (we did not examine its cybersecurity controls. On 1 January 2023, Digital Victoria moved to this department from the Department of Premier and Cabinet)
- Department of Jobs, Skills, Industry and Regions (formerly the Department of Jobs, Precincts and Regions before 1 January 2023)
- Department of Premier and Cabinet
- Department of Health
- Grampians Health Horsham
- Moorabool Shire Council
- Office of the Victorian Information Commissioner
- South East Water.

The report does not identify the agencies in detail due to potential security risks. We have given each agency a detailed management letter about its control weaknesses for its internal reference.

Our audit objective

Are agencies' cloud-based identity management and device management controls effective?

What we examined

We examined if agencies:

- effectively implement identity and device controls for their Microsoft 365 cloud products (see Section 2)
- report on their compliance and secure scores (see Section 2)
- use cybersecurity technology to prevent, detect and respond to risks (see Section 2)
- coordinate to address cybersecurity risks (see Section 3).

We did not examine:

- how agencies secure or use data within their Microsoft 365 products
- other controls outside of the Microsoft 365 products
- Cenitex's and the Department of Government Services' identify and device controls.

Conducting this audit

Assessing performance

To form our conclusion against our objective we used the following evaluation criteria:

Criteria

1.1	Agencies' logical security controls associated with their cloud computing products[1] are consistent with relevant guidance across identity and device elements.
1.2	Agencies report a compliance posture[2] and their secure scores[3] to accountable risk owners.
1.3	Agencies have and use cybersecurity technologies that allow them to improve their cybersecurity.
1.4	Agencies can demonstrate that they have implemented measures to avoid duplication, overlap or fragmentation associated with the security posture of state and local government.

Note:

[1] We looked at Microsoft 365 cloud products in this audit.

[2] Compliance posture refers to agencies' annual compliance attestations to relevant authorities.

[3] Secure scores are agencies' Microsoft Secure Scores.

Our methods

As part of the audit we:

- assessed:
  - 8 agencies' Microsoft 365 cloud products
  - how one agency manages shared Microsoft 365 products
  - how agencies configure identity and device controls
  - the agencies' strategies, policies and procedures for managing their Microsoft 365 cloud products
- interviewed key staff
- contracted subject matter experts to:
  - develop a control library for identity and devices in line with relevant standards and frameworks
  - develop a tool for agencies to self-assess their identity and device controls
  - analyse how agencies have configured their identity and device controls for Microsoft 365 cloud products
  - provide findings based on this analysis.

Compliance

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

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

We also provided a copy of the report to the Department of Treasury and Finance.

Cost and time

The full cost of the audit and preparation of this report was $710,000.

The duration of the audit was 13 months from initiation to tabling.