VAGO
Victorian Auditor-General's Office

Cybersecurity: Cloud Computing Products

August 2023

Independent assurance report to Parliament
2023–24:1

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 for Monza Recycled is cradle to grave including Scopes 1, 2 and 3. It has FSC Mix Certification combined with 99% recycled content.

ISBN 978-1-921060-64-9

VAGO
Victorian Auditor-General's Office

Cybersecurity: Cloud Computing Products

Independent assurance report to Parliament
Published by order, or under the authority,
of the Parliament of Victoria
August 2023

VAGO
Victorian Auditor-General's Office

The Hon Shaun Leane MP
President
Legislative Council
Parliament House
Melbourne

The Hon Maree Edwards MP
Speaker
Legislative Assembly
Parliament House
Melbourne

Dear Presiding Officers

Under the provisions of the *Audit Act 1994*, I transmit my report *Cybersecurity: Cloud Computing Products*.

Yours faithfully

Andrew Greaves
Auditor-General
16 August 2023

The Victorian Auditor-General's Office (VAGO) acknowledges the Traditional Custodians of the lands and waters throughout Victoria. We pay our respects to Aboriginal and Torres Strait Islander communities, their continuing culture, and to Elders past and present.

Contents

Audit snapshot 1

Our recommendations 2

What we found 4

Key finding 1: Overall, audited agencies do not have fully effective Microsoft 365 cloud-based identity and device controls 4

Key finding 2: Not all audited agencies properly understand and oversee cybersecurity services delivered by third-party providers 7

Key finding 3: The public sector does not use its size and economy of scale to address cybersecurity risks in a coordinated way 8

1. Audit context 10

Cyber attacks 10

Cybersecurity 11

Relevant frameworks, roles and responsibilities 15

2. Effectiveness of identity and device controls 17

Agencies do not have fully effective Microsoft 365 cloud-based identity controls 18

Agencies do not have fully effective Microsoft 365 cloud-based device controls 20

Agencies can improve their reporting on cybersecurity 24

Not all audited agencies understand and oversee cybersecurity services delivered by third-party providers 25

3. Whole-of-government approach to cybersecurity 27

Agencies lack a coordinated approach to address cybersecurity risks 27

Appendices 30

Audit snapshot

What we examined

We examined the effectiveness of agencies' Microsoft 365 cloud-based identity and device management controls.

We selected a range of agencies, including government departments, a local council, a water authority, a health service and other entities, to assess their approaches to cybersecurity. We did not examine Cenitex's and the Department of Government Services' controls.

Why this is important

Cybersecurity threats in Victoria are real and growing.

The Department of Premier and Cabinet reported that 90 per cent of Victorian Government agencies experienced cybersecurity incidents last year.

Successful attacks on Victorian Government agencies have seriously disrupted critical services.

It is important that agencies have strong cybersecurity controls to reduce the risk of this happening again.

This includes making sure:

- their identity and device controls are effective
- they only allow authorised users and approved devices access to sensitive information.

What we concluded

The audited agencies' Microsoft 365 cloud-based identity and device controls are not fully effective. They can do more to improve their cybersecurity.

The public sector does not use its size and economy of scale to address cybersecurity risks in a coordinated way.

Agencies have recognised the need to establish a whole-of-government approach. But they need to do more to improve cybersecurity for the entire sector.

What we recommended

We made 2 recommendations to the newly formed Department of Government Services and one recommendation to the Office of the Victorian Information Commissioner to lead a whole-of-government approach to improve the public sector's cybersecurity.

We made 4 recommendations to all the agencies we audited to address control weaknesses and improve their cybersecurity.

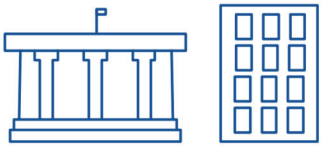
We also made one recommendation about improving agencies' oversight of the cybersecurity services they outsource.

→ Full recommendations

Key facts and findings

90% of Victorian Government agencies experienced a cybersecurity incident in 2022

94%, or 617k, of user accounts at audited agencies are not registered for MFA*



Audited agencies do not have effective Microsoft 365 cloud-based identity and device controls

Note: *Multi-factor authentication (MFA) is a control that requires users to verify their identity using at least 2 methods before they can access an agency's systems or documents.
Source: VAGO based on agencies' information.

Our recommendations

We made 7 recommendations to address 3 key findings. The relevant agencies have accepted the recommendations in full or in principle or with qualifications. While our recommendations are directed to audited agencies, we expect all Victorian public sector agencies to implement them where appropriate.

Key issues and corresponding recommendations			Agency response(s)
Issue: The public sector lacks a coordinated approach to address cybersecurity risks			
Department of Government Services and Office of the Victorian Information Commissioner	**1**	Work together, in consultation with other relevant agencies, to issue non-overlapping guidance that: • streamlines fragmented reporting requirements • balances security and productivity • does not create unintended consequences, such as multi-factor authentication fatigue. The guidance should mandate: • conditional access policy and device compliance policy configurations • additional technical control configurations consistent with the maturity model in this report • an issuer of device security configuration baselines. This mandate should apply to all classes of identities and devices used to access public sector resources, including but not limited to personal computers, mobile devices, guest users, ordinary users, privileged users, service accounts and non-human identities. Agencies should report their compliance against the issued guidance to their accountable risk owners and audit and risk committees at least annually (see Section 3).	Accepted by the Department of Government Services Accepted with qualifications by the Office of the Victorian Information Commissioner
Department of Government Services	**2**	Extends the cyber hubs and the security operation centres to: • maximise the number of Victorian public sector agencies protected • include protection services against cyber attacks (see Section 3).	Accepted in principle

Key issues and corresponding recommendations			Agency response(s)
All audited agencies that are not using a security operation centre	**3**	Complete an independent (internal or external) risk assessment to inform whether they need a security operation centre to improve their cybersecurity and report the results of this assessment to their accountable officer and audit and risk committee. The risk assessment should: • identify the current gaps in their compliance and security posture as per the Victorian Government guidance and global standards • assess the capability and capacity of their cybersecurity team's knowledge, skills and resources (see Section 3).	Accepted by all applicable agencies
Issue: Audited agencies do not have fully effective Microsoft 365 cloud-based identity and device controls			
All audited agencies	**4**	Address the technical compliance control configuration weaknesses we detailed in each agency's management letter (see Section 2).	Accepted in principle by the Department of Education Accepted by all other applicable agencies
	5	Report the following to accountable risk owners at least quarterly: • their Microsoft Secure Score • a breakdown of controls completed by native solutions, third-party solutions and alternative mitigations • an adjusted Microsoft Secure Score that reflects the effectiveness of controls implemented by third-party solutions and alternative mitigations (see Section 2).	Accepted by all applicable agencies
	6	Ensure accountable risk owners document their risk acceptance for controls marked as risk accepted, resolved via third-party solutions or alternative mitigations (see Section 2).	Accepted by all applicable agencies
Issue: Audited agencies insufficiently oversee cybersecurity services delivered by third-party providers			
All audited agencies who use third-party services	**7**	Oversee and ensure that: • the services they buy from third-party providers meet their cybersecurity requirements • third-party service providers have implemented the controls they are responsible for • the implemented controls are effective (see Section 2).	Accepted by all applicable agencies

What we found

This section summarises our key findings. Sections 2 and 3 detail our complete findings, including supporting evidence.

In this report we do not specify which findings relate to which agency given the sensitive nature of the weaknesses we observed. But we have given each audited agency a detailed report about their own control deficiencies.

When reaching our conclusions, we consulted with the audited agencies and considered their views. The agencies' full responses are in Appendix A.

Why cybersecurity is important

A successful cyber attack can harm the community and cause severe damage.

This is because an attack can:

- cause personal data breaches
- disrupt communication networks
- shut down water, health and other critical facilities.

The Victorian Government considers cybersecurity to be one of the top 10 risks for the state.

It became even more important for organisations to have effective cybersecurity controls when Victorians started working from home during the COVID-19 pandemic.

This is because staff often use their own internet service to connect to agencies' networks.

Our key findings

Our findings fall into 3 key areas:

1	Overall, audited agencies do not have fully effective Microsoft 365 cloud-based identity and device controls.
2	Not all audited agencies properly understand and oversee cybersecurity services delivered by third-party providers.
3	The public sector does not use its size and economy of scale to address cybersecurity risks in a coordinated way.

Key finding 1: Overall, audited agencies do not have fully effective Microsoft 365 cloud-based identity and device controls

Why effective identity and device controls are important

Identity and device controls are the first 2 pillars of the zero trust model. These cybersecurity controls help agencies:

- make sure only authorised users and approved devices can access sensitive information
- comply with recommended security frameworks and standards.

The zero trust model's 6 pillars

Identities, devices, applications, data, infrastructure and networks are 6 foundational elements, or pillars, that make up modern information technology (IT) operations.

The zero trust model is a high-level strategy. It assumes that users, devices and services attempting to access resources, even from inside the network, cannot automatically be trusted.

Effective identity and device controls

We developed a list of best-practice compliance controls for identity and devices. We used this list to assess the maturity of agencies' cybersecurity controls.

The list does not include all applicable identity and device controls. We selected controls based on relevant frameworks and standards, which Section 1 details.

The list is a good starting reference for agencies to understand what best-practice compliance looks like. It can help agencies identify gaps in how they manage their identity and device controls.

Identity controls

We assessed 33 identity controls. None of the agencies have fully implemented all these controls. Specifically:

We assessed if agencies ...	Out of 8 agencies we looked at, we found ...
have a centralised identity and access management (IAM) system.	• 7 agencies have a centralised IAM system • the agency that does not have a centralised IAM system is in the final stages of implementing one.
have controls for managing privileged access.	• 4 agencies give users the lowest possible access they need to do a task, which is technically known as least-privilege access • only 2 agencies use privileged access devices for highly privileged roles • none of the agencies have implemented all 6 privileged access controls we assessed.
require strong user authentication methods.	• only half of the agencies require multi-factor authentication (MFA) for all users • none of the agencies use passwordless authentication.
set up conditional access policies for identity.	• only one agency has appropriately set up all 7 conditional access policies for identity.

Privileged access management

Agencies can give some users access to more functions than standard users, such as accessing, modifying or deleting sensitive information as well as making changes to servers, devices and user accounts.

MFA

MFA is a control that requires users to verify their identity using at least 2 methods before they can access an agency's systems or documents.

Passwordless authentication

Passwordless authentication lets a user access an application or IT system without entering a password. Instead, the user may log in with passwordless technology, such as biometrics.

This reduces the risk of people relying on remembering passwords to access systems.

Conditional access policies

Agencies can implement conditional access policies to require a user to complete an action if they want to access their networks.

Device controls

We assessed 22 device controls. None of the agencies have implemented all these controls. Specifically:

We assessed if agencies ...	Out of 8 agencies we looked at, we found ...
set up conditional access policies for devices.	• 7 agencies have not set up any conditional access policies for devices.
have and use cybersecurity solutions.	• all the audited agencies have cybersecurity tools, but not all use native solutions • they do not always actively use data from these tools to prevent, monitor and detect risks.
define and implement configuration policies that include: • security configuration baselines • compliance policies.	• 4 agencies do not have an approved security configuration baseline • of the 4 agencies that have a security configuration baseline, 2 do not monitor if devices comply with these baselines • 4 agencies do not have a defined compliance policy.

Cybersecurity solution

Modern cybersecurity solutions use technology such as threat and artificial intelligence to analyse user behaviours and other signals. These solutions can be used to detect and respond to threats.

A native cybersecurity solution is one from the cybersecurity platform provider, such as Microsoft.

Security configuration baseline

A security configuration baseline is the recommended settings that an agency can use to set up its devices.

Compliance policy

A compliance policy is a set of rules that a device must comply with. For example, an agency may require devices to have antivirus software.

Impact of ineffective identity and device controls

Without effective identity and device controls agencies are more susceptible to cyber attacks.

This is because agencies cannot stop malicious users from using unsecured accounts and noncompliant devices to access their networks.

Reporting on compliance and security posture

All audited agencies have assigned risk owners for their cybersecurity risks and report emerging risks to their relevant committees.

We assessed if agencies report their ...	Out of 8 agencies we looked at, we found ...
compliance against the *Victorian Protective Data Security Standards*.	• one agency does not give its annual attestation against the *Victorian Protective Data Security Standards* to its audit and risk committee for review.
Microsoft Secure Scores (secure scores) to accountable risk owners.	• 2 agencies report their secure scores regularly to their senior leadership • 6 agencies have secure scores over 75 per cent, which is Digital Victoria's recommended minimum secure score.

An agency's secure score indicates its security posture in the Microsoft 365 cloud environment.

Secure scores are automatically calculated using monitoring technology that scans an agency's environment. But if an agency uses a third-party solution or an alternative mitigation, a secure score may not accurately reflect if the agency has adequately set up a control.

Of the 8 audited agencies, each agency implemented an average of 180 out of 1,072 (17 per cent) controls using third-party solutions and alternative mitigations.

This means that:

- the reported secure scores may not accurately reflect an agency's true security posture
- agencies cannot solely rely on their secure scores to monitor their security posture. Agencies need to confirm if their controls that use third-party solutions and alternative mitigations have been set up properly.

Key finding 2: Not all audited agencies properly understand and oversee cybersecurity services delivered by third-party providers

Why it is important

An agency can use a third-party service provider to manage their cybersecurity services.

But the agency is accountable for its overall cybersecurity risks. This is because an agency cannot delegate its accountability to a third-party provider.

Being accountable for cybersecurity risks means that an agency should:

- be clear about the roles and responsibilities it has under:
  - shared service arrangements
  - managed service arrangements
- regularly review and ensure the controls implemented in both arrangements meet the agency's requirements and address its cybersecurity risks.

Shared service arrangement

Under a shared service arrangement, the service provider determines and implements controls. An agency needs to assess if the controls meet its requirements before entering the engagement.

Managed service arrangement

Under a managed service arrangement, the agency determines and oversees the controls. The service provider is responsible for implementing them.

Cenitex-managed shared services and products

Cenitex manages a suite of Microsoft 365 products. Many government agencies use and share these products and services.

Cenitex can play different roles depending on how agencies want to engage with it.

When Cenitex is the cloud service provider under a shared service arrangement:

- Cenitex is the owner of the shared products and services and is responsible for determining and configuring cybersecurity controls for the Microsoft 365 tenancy
- agencies are users, not owners, of these products and therefore are only responsible for their data in the Microsoft 365 tenancy.

Agencies are not clear about their security roles and responsibilities under the shared service arrangement.

For example, some agencies who are part of the shared tenancy think they are the owners of the tenancy and should be able to determine and configure cybersecurity controls.

Agencies, as users of the tenancy, should:

- periodically review if controls for Cenitex's Microsoft 365 tenancy meet their cybersecurity requirements
- identify if they need to implement additional controls to address any identified gaps and assess if:
  - these controls can be implemented by Cenitex
  - agencies need to set up controls of their own outside of the tenancy to mitigate their cybersecurity risks.

If these options are not possible, agencies should consider other suitable arrangements.

Microsoft 365 tenancy

A Microsoft 365 tenancy is a dedicated environment within the Microsoft 365 cloud. It provides a range of services from Microsoft.

When an agency buys a Microsoft 365 subscription, it is allocated to a tenancy. Agencies can share a tenancy.

Impact of unclear roles and insufficient oversight

There could be potential gaps in agencies' cybersecurity controls because they:

- have an unclear understanding of their roles
- do not sufficiently oversee the shared services.

Key finding 3: The public sector does not use its size and economy of scale to address cybersecurity risks in a coordinated way

Why a coordinated approach is important

Audited agencies have different levels of maturity for cloud-based identity and device controls.

Agencies recognise that:

- cybersecurity skills are distinct from general IT skills
- preventing, detecting and responding to cyber attacks requires a multidisciplinary team with expertise across different security functions.

As agencies move away from on-premises computing to cloud computing platforms, they are also increasingly changing their control configurations from agency-specific settings to universal uniformed ones. This means that the identity and device control options for agencies will become well defined and near identical.

Agencies do not always have the resources to establish cybersecurity teams with up-to-date knowledge and skills. But they could benefit from a whole-of-government approach to implement these controls to improve their cybersecurity.

Proposed cyber operating model

In November 2020, the Department of Premier and Cabinet established Digital Victoria to support digital transformation across the Victorian Government. Digital Victoria moved to the Department of Government Services on 1 January 2023.

Digital Victoria aims to guide and support the public sector to work in a more collaborative way.

Victoria's Cyber Strategy 2021 and its 2021–2023 mission delivery plans recognise the need to build a cyber hubs model to improve the public sector's governance, technology and how it manages resources.

As part of the work to deliver *Victoria's Cyber Strategy 2021*, Digital Victoria asked agencies to voluntarily share their Microsoft Secure Score data so it could:

- analyse agencies' cybersecurity
- identify which agencies need extra support
- identify what areas agencies need further training in.

However, not all agencies agreed to share their data. This is because Digital Victoria has no legal authority to issue mandatory guidance and request information.

As a result, although 150 agencies agreed to participate in the program, Digital Victoria was only able to analyse the data from 40 agencies who shared their data.

This means Digital Victoria:

- does not have full visibility of agencies' cybersecurity data
- cannot identify systemic issues or concerns across the sector.

This may affect Digital Victoria's ability to deliver the whole-of-government cyber operating model.

Using centralised SOCs

We found that not all agencies use centralised security operation centres (SOCs).

A SOC is an in-house or outsourced team of IT security professionals that monitors an agency's IT systems 24/7 to:

- detect cybersecurity risks in real time
- respond to risks of attacks as quickly and effectively as possible.

The health sector set up its SOC in 2020. This is a good example of agencies detecting and responding to cybersecurity risks using a centralised solution.

Under the 2021–2023 mission delivery plans, Digital Victoria aims to set up centralised SOCs for agencies, including government departments and entities and local government authorities.

However, the current SOC arrangements do not provide services for agencies to protect against cyber attacks. This means that individual agencies are delivering this function independently.

It is often challenging for individual agencies to have the necessary resources and scale to establish cybersecurity teams with up-to-date knowledge and skills.

This gap in the arrangements can expose agencies to high cybersecurity risks.

Impact of not having a coordinated approach

There are over 3,000 entities that deliver services to the public.

Without a coordinated approach, many agencies are duplicating their efforts and not using the public sector's economy of scale to efficiently manage cybersecurity risks.

1. Audit context

Cyber attacks

Impact of cyber attacks

Public sector agencies are constantly at risk of cyber attacks.

Microsoft reports and analyses 43 trillion threat signals for its cloud computing products every day.

Cyber attacks can:

- cause data breaches of:
  - personal information
  - confidential information about organisations
- interrupt the availability of IT systems, which can lead to agencies not being able to provide critical services.

Figure 1 shows a number of recent high-profile cyber attacks that impacted critical infrastructure.

Figure 1: Recent high-profile cyber attacks that impacted critical infrastructure

 2019 Victorian hospital cyber attacks	In September 2019 multiple hospitals in Victoria experienced a cyber attack. Malicious users installed software that made booking systems unusable for more than 24 hours. While no patient information was leaked, it delayed surgeries.
 2021 USA Colonial Pipeline shutdown	In 2021 malicious users accessed America's largest oil pipeline using a staff member's leaked password. After stealing 100 GB of data, the attackers installed software that blocked Colonial Pipeline's access to its IT network. Colonial Pipeline had to shut down production to stop the software spreading. This led to petrol shortages, which caused airline and freight delays and increased the price of petrol globally.
 2022 Costa Rica state of emergency	In May 2022 Costa Rica's government declared a state of emergency after malicious users got access to the government's IT network using a leaked password. After stealing sensitive financial information, the malicious users installed software that shut down critical financial systems. This stopped the government from paying its workers and disrupted its tax and customs systems. As a result, Costa Rica's import and export logistics collapsed, which made the government lose US$30 million per day.
 2022 Australian Optus data breach	Most attacks in Australia cause data breaches, including the Optus cyber attack in 2022. In this attack, malicious users got Optus customers' information using software that did not require authentication to access. The malicious users stole 10 million past and existing customers' addresses and driver licence numbers. State governments were forced to reissue licences due to the heightened risk of identity theft.

2022 Fire Rescue Victoria data breach	In December 2022 Fire Rescue Victoria reported a cyber attack that impacted a number of its communications systems. On top of data breaches of current and previous staff's personal information, data about people who had applied for positions was also leaked. The cyber attack caused an outage of Fire Rescue Victoria's computer dispatch system and phone lines. This left firefighters having to rely on alerts about emergencies directly from their mobile phones or radio messages.
2023 Tasmanian Government data breach	In April 2023 the Tasmanian Government announced that 16,000 documents had been leaked online due to a cyber attack on its third-party file transfer system. This attack targeted the Tasmanian Department for Education, Children and Young People. Information about students' names, addresses and their families' bank details was compromised.

Source: VAGO from public media.

Who carries out cyber attacks?

There are various types of malicious users with different motivations for carrying out a cyber attack:

Malicious users	Common motivation
Nation-states	Geopolitical
Cybercriminals	Profit
Hacktivists	Ideological
Terrorist groups	Ideological violence
Thrill-seekers	Satisfaction
Insider threats	Discontent

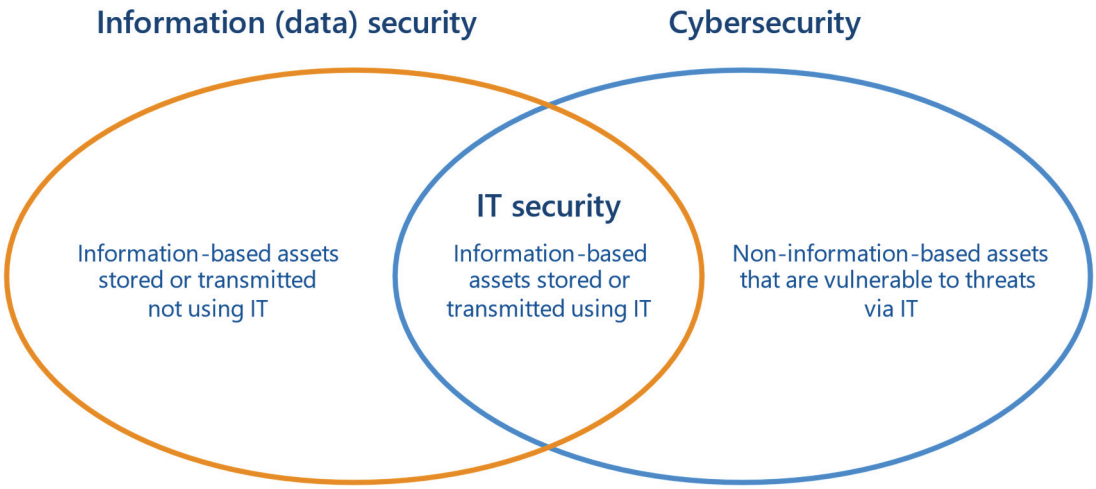
Cybersecurity

What is cybersecurity?

An agency's cybersecurity or cybersecurity posture is its ability to identify, protect, detect and respond to cyber attacks.

Cybersecurity is different from IT or data security. Figure 2 shows the differences.

Figure 2: Differences between cybersecurity, information security and IT security



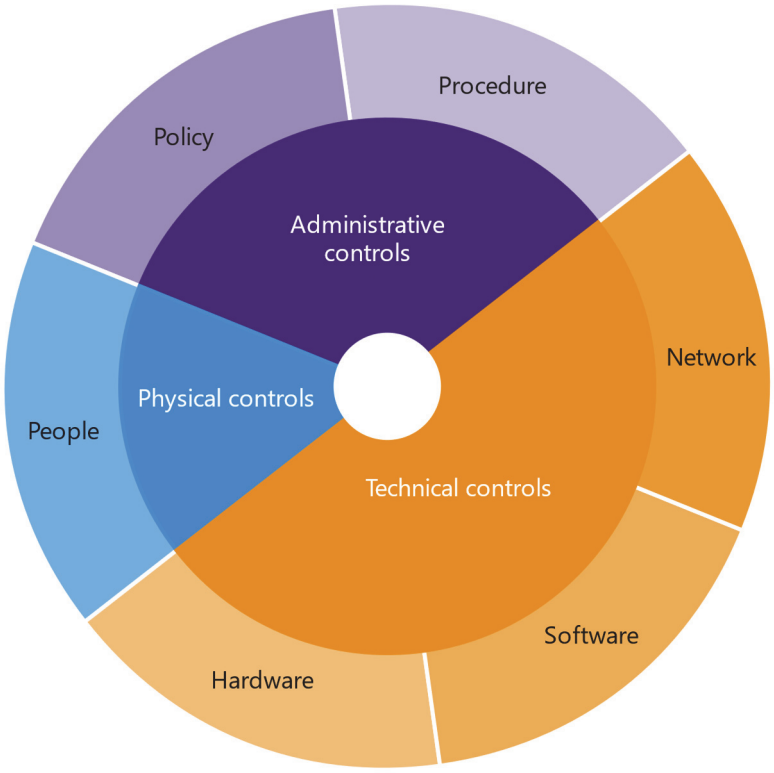
Source: VAGO based on information from industry standards.

Improving cybersecurity

As Figure 3 shows, an agency can improve its cybersecurity by having strong:

- technical controls, including system configurations
- administrative controls, including frameworks, policies, guidelines and processes
- physical controls, which are tangible methods of preventing or detecting unauthorised access to a system.

Figure 3: Types of cybersecurity controls



Source: VAGO based on information from industry standards.

Without correct system configurations, an agency cannot reduce its cybersecurity risks, despite having good administrative and physical controls.

Well-configured technical controls achieve a balance of security and productivity.

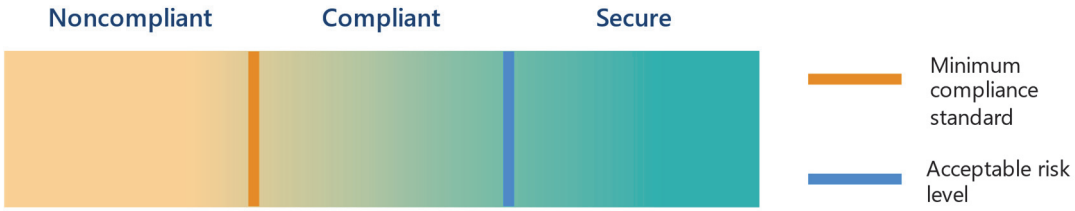
This audit focuses on agencies' technical controls – their system configurations for the Microsoft 365 environment.

Compliance and security

There are 2 important concepts for measuring technical controls – compliance and security, which Figure 4 shows.

Compliance focuses on meeting industry standards. Security goes beyond compliance. It is about implementing measures to reduce the risks of cyber attacks to an acceptable level.

Figure 4: Compliance vs. security



Source: VAGO based on information from industry standards.

This audit focuses on how agencies' technical controls align with best practice compliance.

How the cloud improves cybersecurity

The fourth industrial revolution is the next phase of digitising the workforce. It is driven by improvements in data, connectivity and technology.

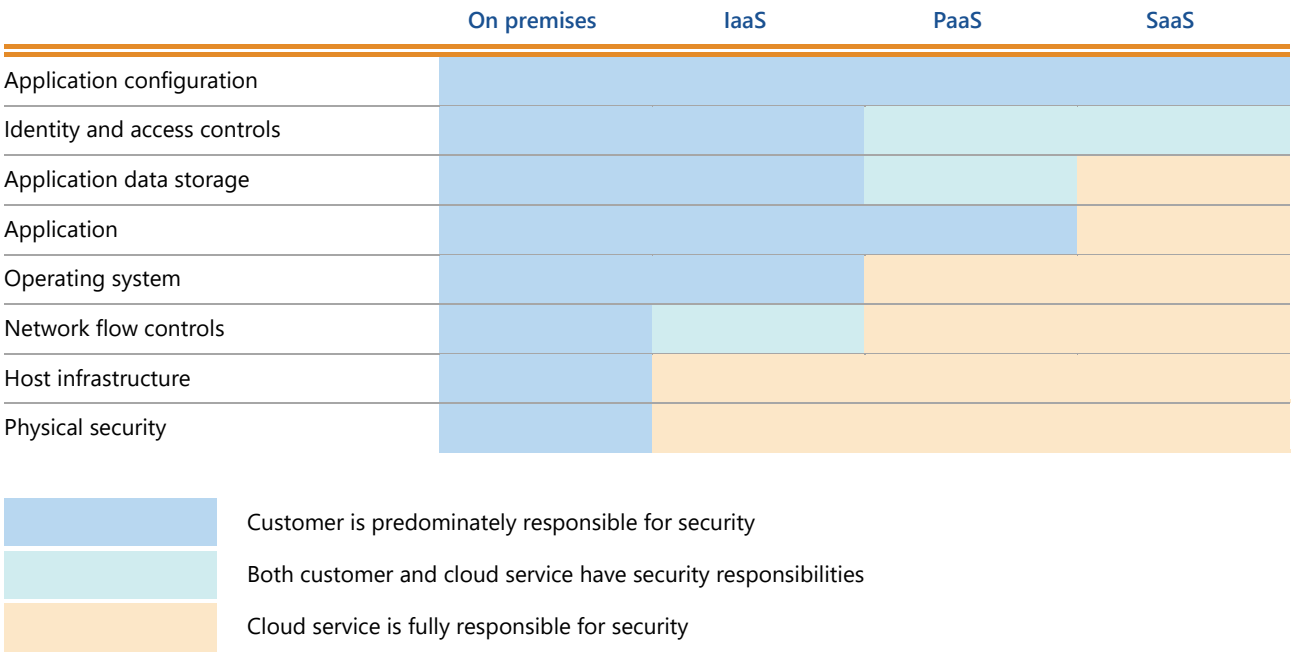
Cloud computing is essential to the fourth industrial revolution. It allowed Victorian public sector agencies to work remotely during the COVID-19 pandemic.

The cloud can improve an agency's cybersecurity if it is configured effectively. This is because it:

- shifts cybersecurity responsibilities to cloud providers, which frees up agencies' resources
- leverages the cloud provider's security capabilities for extra protection
- uses information from cloud providers to improve detection and response times to cyber threats.

Figure 5 shows the allocation of responsibilities for the 4 main cloud security types.

Figure 5: Shared responsibility model



Note: IaaS stands for infrastructure as a service, PaaS stands for platform as a service, and SaaS stands for software as a service.
Source: VAGO based on the Australian Cyber Security Centre's 2022 cloud security guidance.

Cloud service providers

Common cloud service providers include:

- Microsoft 365 and Microsoft Azure
- Amazon Web Services
- Google Cloud Platform.

The cloud

The cloud is when a service provider supplies software, data storage and other services over the internet.

The cloud is more economical, effective and efficient compared to traditional computing, which relies on in-house servers and databases.

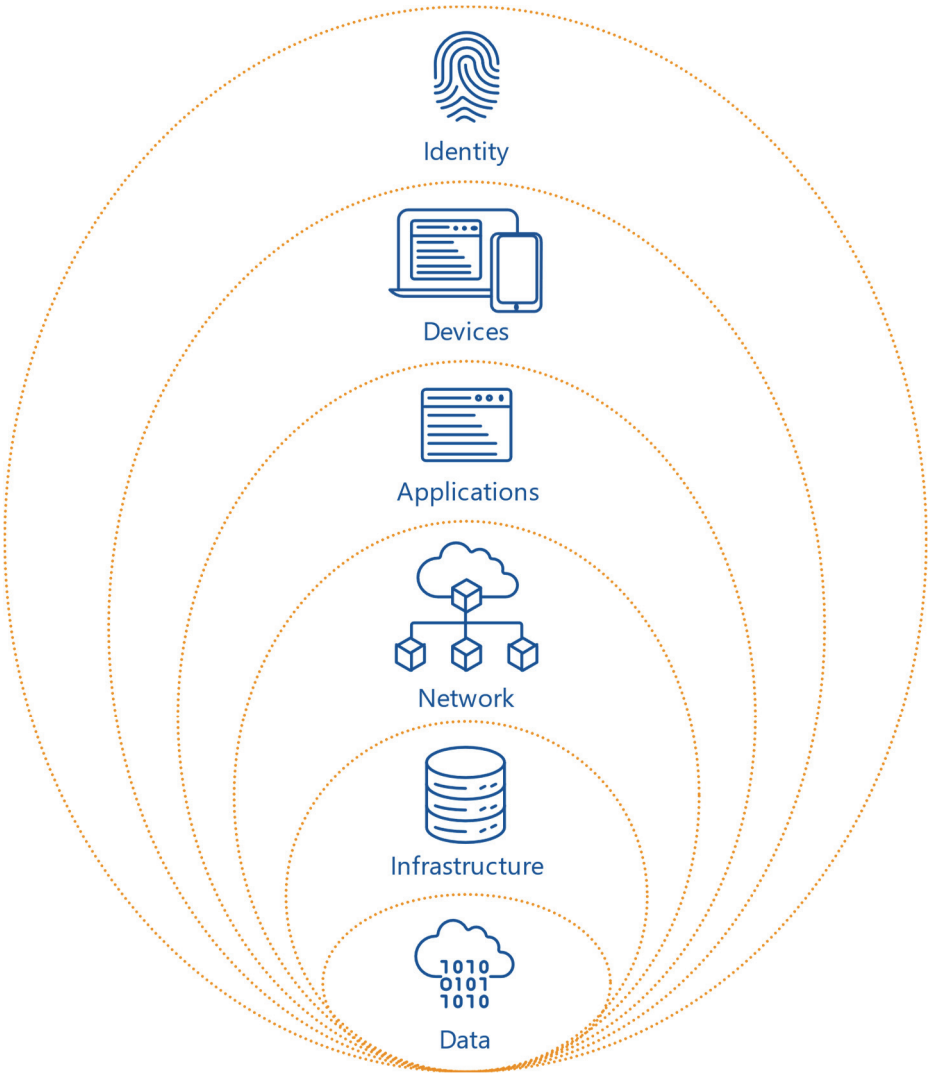
Zero trust

Zero trust is the concept of not trusting anything inside or outside an agency's network.

Under a zero trust model, an agency's IT system explicitly verifies users and devices before they can access resources. Zero trust creates a secure environment that protects against unauthorised access to sensitive data.

The zero trust model applies to 6 key pillars, which Figure 6 shows.

Figure 6: The 6 pillars of zero trust



Source: VAGO based on information from Microsoft.

This audit looks at identity and device controls.

Relevant frameworks, roles and responsibilities

Cybersecurity standards and frameworks

Many globally recognised organisations have published standards and frameworks for improving cybersecurity. These include:

Organisation	Standards or frameworks
Australian Cyber Security Centre	• *Information Security Manual* • *Essential Eight*
Center for Internet Security (CIS)	*CIS Critical Security Controls*
Defence Information Systems Agency (DISA)	Security technical implementation guides
Microsoft	Microsoft Cloud Security Benchmark documentation (MCSB)
National Institute of Standards and Technology	*NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations*
Office of the Victorian Information Commissioner	• *Victorian Protective Data Security Standards* (2019) • *Victorian Protective Data Security Framework* (2020)
Payment Card Industry Security Standards Council	*Payment Card Industry Data Security Standard*

These standards and frameworks are comprehensive. But they have a lot of overlap and all point to similar technical configurations.

Organisations have mapped some of the similarities and differences between the standards. However, understanding the dynamics between each standard and identifying which controls to implement can require additional effort and costs for agencies.

Microsoft's MCSB aims to harmonise the already published standards and frameworks to provide a single, comprehensive controls framework for Microsoft 365 products.

The National Office of Cyber Security

In December 2022 the Australian Government announced it is developing the 2023–2030 Australian Cyber Security Strategy. The strategy will aim to make Australia the most cyber-secure nation by 2030. It has led to the Australian Government setting up the National Office of Cyber Security.

The Australian Government has also appointed a coordinator in June 2023 who is responsible for improving Australia's cybersecurity and resilience.

Agencies who have a role in cybersecurity in the Victorian public sector

A number of entities play a role in improving cybersecurity for the Victorian public sector, including:

	Is responsible for …	**And it released …**
The Victorian Government	setting out the government's digital vision and ambition and direction for agencies to realise it	*Victorian Government Digital Strategy 2021–2026*.
Digital Victoria (part of the Department of Government Services)	supporting the Victorian public sector's digital transformation	• *Victoria's Cyber Strategy 2021* • 2021–2023 mission delivery plans • *Victorian Government Office 365 Security Guidance* (2022).
The Office of the Victorian Information Commissioner	being the primary regulator and a source of independent advice to the community and Victorian Government about how the public sector collects, uses and discloses information	• *Victorian Protective Data Security Framework* (2020) • *Victorian Protective Data Security Standards* (2019).
Digital Health (part of the Department of Health)	overseeing the health sector's cybersecurity by working closely with the Victorian Managed Insurance Authority	a health sector cybersecurity assessment tool in 2018.

2. Effectiveness of identity and device controls

Agencies are not adequately prepared to prevent cyber attacks. This is because they have not correctly configured all of their Microsoft 365 cloud-based identity and device controls.

Why identity and device controls are important

Identity and device controls are 2 pillars of the zero trust model. These controls help an agency:

- make sure only explicitly verified users and devices can access its systems
- meet relevant compliance frameworks and standards.

Without strong identity and device controls, agencies are more at risk of cyber attacks.

Well-configured controls achieve a balance between productivity, or how quickly a person can access the resources they need, and cybersecurity.

For example, passwordless authentication:

- removes the need for users to remember and input different passwords
- is more secure, as passwords can be guessed.

This improves productivity because there are fewer prompts to input passwords for users.

Effective identity and device controls

We developed a list of best-practice compliance controls for identity and devices. We assessed agencies against this list. The list focuses on technical controls, not physical or administrative controls.

The list does not include all applicable identity and device controls. We selected these controls based on:

- relevant frameworks and standards
- implementation guidance from cloud computing product providers.

We list these frameworks, standards and guidance in Section 1.

Our list can help agencies identify gaps in how they manage their identity and device controls.

We gave each agency a personalised management letter with specific findings about its controls.

Agencies do not have fully effective Microsoft 365 cloud-based identity controls

Identity controls

We assessed 33 identity controls, which Figure 7 shows.

All audited agencies can improve their cybersecurity by correcting the configuration of their identity controls.

Types of users

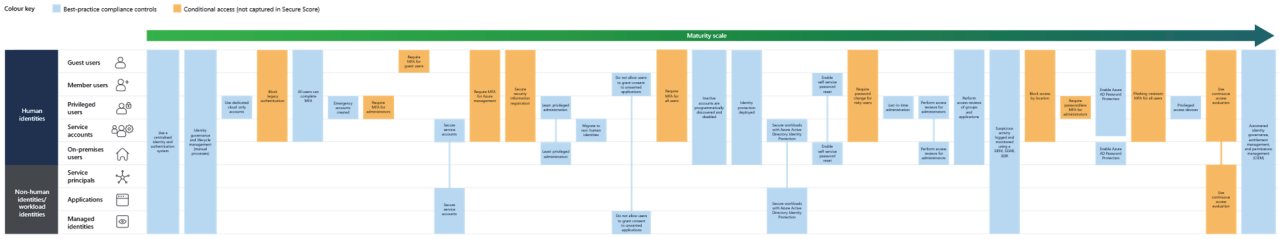
Agencies need to apply different identity controls depending on the user type because of their varying risks.

Common types of users include:

User type	Description
Guest user	A user who is outside of an agency
Member user	A user who is part of an agency
Privileged user	A user who is part of an agency and has access to more functions than a standard user

For example, privileged users can perform security-relevant functions, so agencies need to apply more controls for these users.

Figure 7: Maturity of agencies' identity controls



Note: See the next page for a full-page copy of Figure 7.
See Appendix B for full spelling of acronyms. As we assessed agencies' Microsoft 365 controls, the maturity model uses language from Microsoft's documentation.
Source: VAGO.

IAM systems

Agencies use an IAM system to manage users' access to their IT systems.

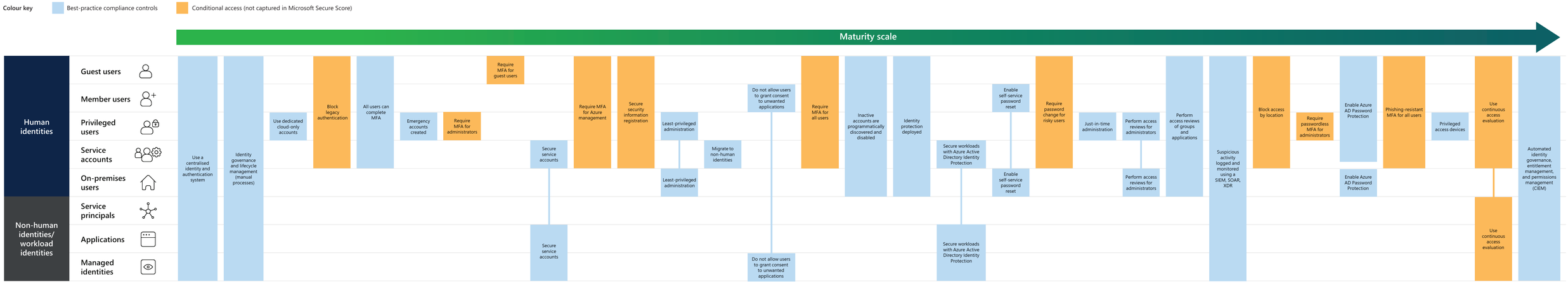
A centralised IAM system:

- protects the confidentiality, integrity and availability of government information
- makes agencies more efficient. For example, when an agency creates a new user in its human resource system it triggers a creation of an account in their IAM system to match the record.

Seven out of 8 agencies have a centralised IAM system. The agency that does not have a centralised IAM system is in the final stages of implementing one.

It is positive that all audited agencies recognise the benefits of having a centralised IAM system.

Figure 7: Maturity of agencies' identity controls



Privileged access management

Agencies should use privileged access management principles to manage, control, and monitor access to important resources.

Malicious users often target weaknesses in privileged user accounts to access an agency's network. This is because these accounts have higher-level permissions. So it is important for agencies to apply privileged access management principles to secure these accounts.

We found that 4 agencies fully use least-privileged administration to manage privileged accounts, which is good practice. The other 4 agencies are in the process of fully implementing it. However:

We found ...	Which ...
only 4 agencies regularly review privileged users	involves making sure that privileged users have an appropriate access level.
only 2 agencies have approval processes to activate highly privileged roles (accounts that have access to more security settings than a regular privileged role)	involves only activating privileged roles when required.
• only 3 agencies have at least 2 emergency access accounts • 2 agencies have only 1 account created • the other 3 agencies have not set up an emergency access account	are highly privileged accounts to help agencies respond to a security emergency.
only one agency uses dedicated cloud-only administration accounts	are accounts that agencies use to change their cloud environment settings.
no agencies have privileged access devices	are devices agencies only use to do sensitive tasks.

Authentication methods

Agencies should set strong authentication controls for their users to reduce the likelihood of cyber attacks.

All audited agencies can improve their authentication controls. For example, by configuring strong authentication methods, such as passwordless authentication, which no agency has configured yet.

MFA requires users to verify their identity using at least 2 methods before they can access an agency's systems or documents. Only 4 agencies require MFA for all users.

According to Microsoft:

- authentication via a text message is not secure
- it is best practice is to use passwordless authentication.

Passwordless authentication is convenient for users. It can also protect an agency's cybersecurity by letting a user access an application or IT system without entering a password or answering security questions. Instead, the user may log in with passwordless technology, such as a mobile phone authentication app, hardware security keys or biometrics.

All audited agencies can increase their authentication methods by implementing the authentication controls in Figure 7.

Case study: One agency has not set up MFA for 48 per cent of its Microsoft 365 users.

The agency told us this is because this user group can experience significant difficulties with MFA.

When we asked what the impact would likely be if this group's accounts got compromised, the agency could not tell us. The agency confirmed that it has not conducted a comprehensive risk assessment to inform the accountable cybersecurity risk owner about:

- the likelihood and impact of the information being breached
- if the perceived 'difficulties' outweigh the implications of the accounts being compromised.

The number and severity of cyber attacks are increasing. So agencies cannot skip a significant control only because it is difficult to implement.

Conditional access policies for identity

An agency can configure conditional access policies to continuously verify each attempt to access its network using signals, such as a user's location, application and device types.

For example, an agency can block an account based on its login location. This is a simple conditional access policy that helps the agency identify and prevent suspicious accounts from accessing its systems from an unusual location.

Agencies with conditional access policies require users to complete an action when they need to access a resource. For example:

If staff log in with a device that is assigned to them and on a network that is ...	**Then the staff ...**
compliant	may bypass MFA.
noncompliant	must complete MFA.

We looked at 5 conditional access policies for identity.

Only one agency uses all these controls appropriately.

All audited agencies can improve their implementation of conditional access policies.

Agencies do not have fully effective Microsoft 365 cloud-based device controls

Device controls

We assessed 22 device controls, which Figure 8 shows. All audited agencies can improve their cybersecurity by correcting their configuration of device controls.

Types of devices

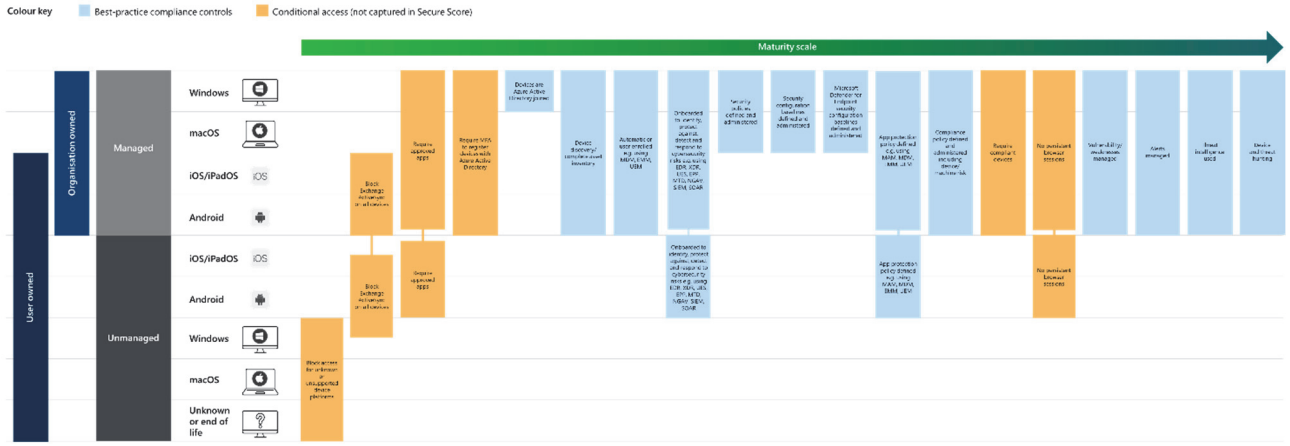
The different types of devices are:

Device type	**Description**
Workstations	Includes desktops and laptops that can run operating systems, such as: • Windows • MacOS
Mobiles	Includes mobile phones and tablets that can run operating systems, such as: • Android • iOS

Some agencies enable staff to work remotely on their own devices, which is known as bring your own device (BYOD). Agencies need to configure relevant controls to ensure these devices do not expose them to malicious users.

For example, agencies should, at a minimum, manage the applications users have in BYODs to ensure they comply. However, we found that most agencies have not focused on managing BYODs, so our findings relate to devices owned by agencies.

Figure 8: Maturity of agencies' device controls



Note: See the next page for a full-page copy of Figure 8.
See Appendix B for full spelling of acronyms. As we assessed agencies' Microsoft 365 controls, the maturity model uses language from Microsoft's documentation.
Source: VAGO.

Conditional access policies for devices

Similar to conditional access policies for identity, an agency can configure conditional access polices for its devices to make sure they meet certain requirements before accessing its systems.

For example, an agency might stop devices that do not have antivirus software installed from accessing its network.

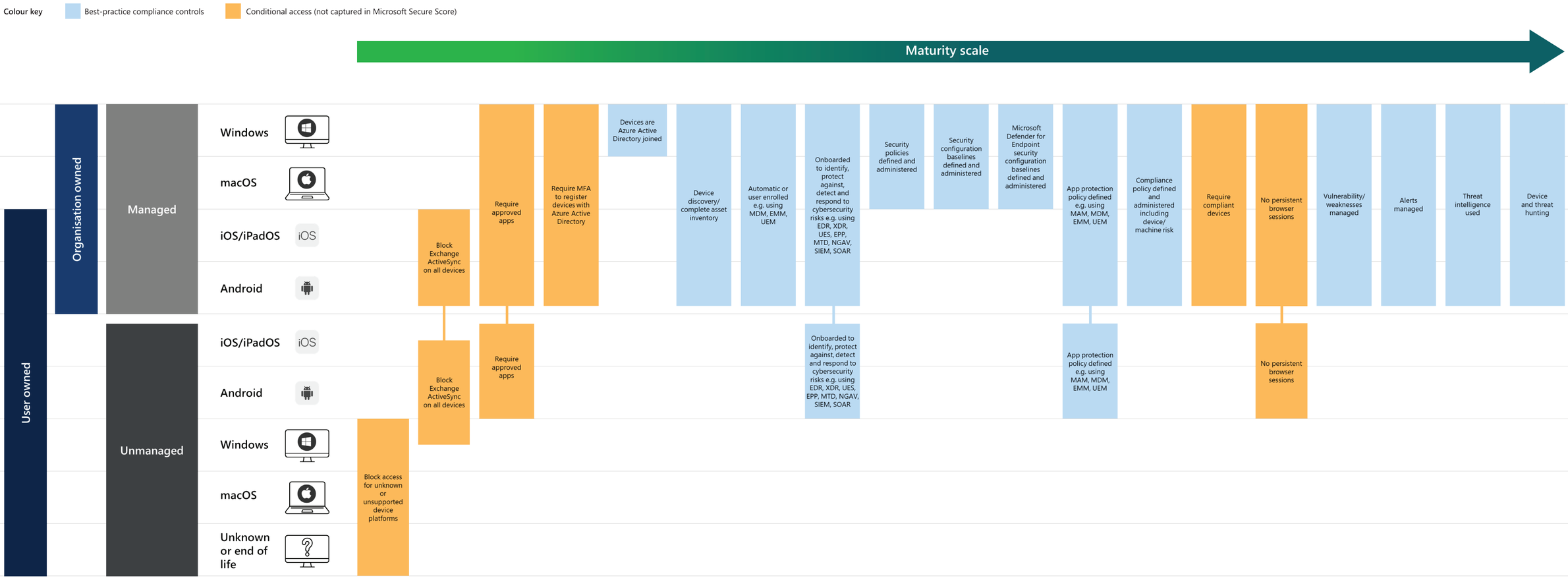
To set conditional access policies for devices, agencies can:

- use a default policy issued by their cloud provider
- develop their own rules.

We assessed …	Out of the 8 agencies, we found …
5 conditional access policies for devices.	• one agency uses 2 policies correctly • none of the other agencies have set up these policies.
if agencies define compliance policies and monitor device compliance status.	• 4 audited agencies have not defined compliance policies for any of their devices • the other 4 agencies that have defined compliance policies can all improve how they administer them. For example, agencies should apply compliance policies to all devices and regularly monitor and report on their compliance status.

None of the agencies have a control to block users with noncompliant devices from accessing their network. This could mean malicious users can take advantage of the vulnerabilities of these devices to access agencies' systems.

Figure 8: Maturity of agencies' device controls



Security configuration baselines

Security configuration baselines are minimum requirements necessary for an information system to maintain an acceptable level of risk.

Agencies, such as CIS and DISA, issue widely accepted best-practice security configurations for different cloud provider products, devices and other services.

Agencies should use best-practice security baselines but can customise some settings to suit their operating environment.

If agencies customise settings, they should clearly document any changes they have made to the best-practice baseline. This can help risk owners track and make sure they accept the consequences of any deviations.

We found ...	**This means that ...**
one agency has not considered using a security configuration baseline.	They do not know if they have their workstations and mobiles configured in line with best practice.
3 agencies have implemented a customised security configuration baseline but they have not sought approval from their risk owners.	Their risk owners have not assessed if they accept the consequences of these deviations.
of the 4 agencies that have security configuration baselines, 2 do not monitor if devices comply with these baselines.	They do not know if their devices are configured in accordance with their security configuration baselines.

Case study: One agency has a documented approval process for customising security configuration baselines. This is better practice.

One agency configures its devices based on Microsoft's security configuration baseline.

The agency has deviated from the baseline in some instances so it can customise some controls. But the agency has clearly documented:

- why the recommended settings were not fit for purpose
- what changes it made
- who approved the changes.

This is an example of better practice because it shows that the agency:

- has used a best-practice baseline as its starting point
- only allows the best-practice baseline to be modified through a robust change control process.

Native cybersecurity solutions

Modern cybersecurity solutions enable agencies to prevent, detect and respond to cyber attack more effectively and efficiently. They leverage methods, such as configuring automated investigation and remediation capabilities, to reduce the time and effort security operations staff need to address a cyber attack alert.

Native cybersecurity solutions are provided by cloud computing platform providers.

We found that not all audited agencies use native cybersecurity solutions. They advised that this is because they already have other solutions that have similar functions.

However:

Agencies with non-native cybersecurity solutions may …	**Because …**
pay extra costs for duplicating tools	some native solutions are already included in the agencies' plans as part of the Victorian Government's licensing agreement with the cloud computing platform providers.
spend more time and effort analysing cybersecurity alerts	non-native cybersecurity solutions: • do not have access to insights from the trillions of signals captured daily from cloud computing platform providers • are more difficult for agencies to configure controls because each solution is set up differently • cannot automatically consolidate data from different solutions to enable easy reporting to management.

Agencies should consider if using native solutions addresses their cybersecurity risks. If it is not the best outcome, agencies should document their rationale for using non-native solutions.

We examined if the number of devices in agencies' device inventories aligns with their other IT system records.

We found that agencies do not keep their device inventories up to date. Only one agency knows:

- the number of devices it manages
- if it has decommissioned outdated devices.

This is because most agencies use non-native cybersecurity solutions and these solutions do not integrate different data sources automatically. Agencies need to manually reconcile records from different systems and often do not have the time and resources to do this over a large number of inventories.

Case study: One agency's records had a difference of over 15,000 devices.

We found that one agency had over 25,900 devices recorded in its compliance management tool. But its IT device inventory only showed 10,100 devices.

The agency told us that it does not know why the records are different. It said it needs to reconcile its inventory to address the issue.

We found inaccurate asset management records at 6 of the 8 audited agencies. This is because they use a variety of cybersecurity solutions that are not integrated to enable easy reporting.

Further, while all the audited agencies have different tools to get information about their cybersecurity position, they do not always use this information to detect and monitor if unauthorised users and devices are accessing their systems.

For example, all the audited agencies have tools to identify cyber threats. But only one agency actively uses this data to regularly address its risks.

Agencies can improve their reporting on cybersecurity

Reporting on compliance and security posture

It is positive that all audited agencies:

- have assigned risk owners for their overall cybersecurity
- report emerging cybersecurity risks to relevant committees.

We assessed if agencies report on their …	And we found …
compliance against the *Victorian Protective Data Security Standards*	one agency does not provide its annual attestation against the *Victorian Protective Data Security Standards* to its audit and risk committee.
secure scores to accountable risk owners	• 6 agencies have a secure score of over 75 per cent, which is Digital Victoria's recommended minimum secure score • only 2 agencies regularly report their secure scores to senior management.

Secure scores indicate an agency's security position in the Microsoft 365 cloud environment.

Secure scores are automatically calculated using monitoring technology that scans an agency's environment. However, if an agency uses a third-party solution or an alternative mitigation method, the scores may not accurately reflect if a control has been adequately set up.

Of the 8 audited agencies, each agency implemented an average of 180 out of 1,072 (17 per cent) controls using third-party solutions and alternative mitigation methods.

This means that:

- the reported secure scores may not accurately reflect agencies' true security posture
- agencies cannot solely rely on their secure scores to monitor their security position. Agencies need to confirm if their controls that use third-party and alternative mitigation methods have been set up properly.

Not all audited agencies understand and oversee cybersecurity services delivered by third-party providers

Why clear roles and responsibilities are important

An agency can manage cybersecurity risks in-house or use a third-party provider to deliver some services.

But the agency is accountable for its overall cybersecurity risks. This is because an agency cannot delegate accountability to a third-party service provider. This means:

An agency can …	This is called a …	But …
rely on a cloud service provider to provide a system, such as a shared Microsoft 365 tenancy, to store and transmit data.	shared service	The cloud service provider determines and configures the controls for the system. Before using the system, the agency needs to make sure the controls for the system are sufficient to address cybersecurity risks. As a user of the system, the agency needs to periodically assess: • if the controls are sufficient to address any new or changed cybersecurity risks • if it needs to implement additional controls.
use a provider to help it implement and manage some controls.	managed service	the agency needs to determine and oversee the controls set up by the third-party service provider.

Cenitex's role as a service provider

Cenitex manages a suite of Microsoft 365 products. Many government agencies use and share these products and services.

Cenitex can play different roles for these products depending on how agencies engage with it.

When Cenitex is the cloud service provider under the shared service arrangement:

- Cenitex is the owner of the shared products and services so it is responsible for determining and configuring cybersecurity controls for the Microsoft 365 tenancy
- agencies are users, not owners, of these products and are only responsible for their data in the Microsoft 365 products.

Cenitex maintains a controls library. Its clients can ask to see this library and any associated security settings that relate to them. Agencies can use this information to make sure the controls are:

- appropriate for their risk profiles and appetite
- operating effectively.

Each year Cenitex gives its clients a report from an external assurance provider about the effectiveness of the controls it manages.

Cenitex's shared services and products

Agencies are not clear about their security roles and responsibilities under their shared service arrangement with Cenitex.

For example, agencies say they are the owners of the shared Microsoft 365 tenancy and should be able to determine and set up controls.

But the *Information Security Manual* says that a user's roles and responsibilities under a shared tenancy should be to:

- periodically review if controls set up in the tenancy by Cenitex meet its cybersecurity requirements
- identify if it needs to implement additional controls to address any identified gaps and assess if:
    - these controls can be implemented in the tenancy by Cenitex
    - it needs to set up its own controls to mitigate the cybersecurity risks.

If these options are not possible, agencies should consider other suitable arrangements.

If Cenitex and its clients are unclear on who is responsible for determining, implementing and overseeing controls, agencies may not be able to adequately manage their cybersecurity risks.

3. Whole-of-government approach to cybersecurity

The public sector does not use its size and economy of scale to address cybersecurity risks in a coordinated way. Agencies have recognised the need to establish a whole-of-government approach but need to do more to improve the public sector's cybersecurity.

Agencies lack a coordinated approach to address cybersecurity risks

Why a coordinated approach is important

As agencies move away from on-premises computing to cloud computing platforms, they are also increasingly changing their control configurations from agency-specific settings to universal uniformed ones. This means that the identity and device control options for agencies will become well defined and near identical. This can help agencies configure controls easily with reduced effort.

Agencies recognise that:

- cybersecurity skills are distinct from general IT skills
- preventing, detecting and responding to cyber attacks requires a multidisciplinary team with expertise across different security functions.

The Victorian public sector has over 3,000 entities that deliver services to the public.

Without a coordinated approach, many agencies are duplicating their efforts and not using the public sector's economy of scale to efficiently manage cybersecurity risks.

Proposed whole-of-Victorian-Government cyber operating model

Victoria's Cyber Strategy 2021 and its 2021–2023 mission delivery plans recognise the need to:

- set up a whole-of-Victorian-Government operating model to improve how the public sector manages cybersecurity risks
- encourage more agencies to use baseline controls and improve their cybersecurity skills
- build a cyber hubs model to improve the sector's governance, technology and how it manages resources. A central Victorian Government cybersecurity defence centre would support these hubs.

In August 2022 Digital Victoria issued the *Victorian Government Office 365 Security Guidance* as part of *Victoria's Cyber Strategy 2021* and mission delivery plans.

This is Digital Victoria's first effort at leading a whole-of-government approach to address cybersecurity risks.

Digital Victoria also asked agencies to voluntarily share their secure score data with it so it could:

- analyse agencies' cybersecurity
- identify which agencies need extra support
- identify what areas agencies need further training in.

However, not all agencies agreed to share their data. This is because Digital Victoria has no legal authority to issue mandatory guidance and request information.

Although 150 agencies agreed to participate in the program, only 40 agencies voluntarily shared their data. As a result, Digital Victoria could only analyse data of 40 agencies, or 27 per cent of participating agencies.

This means Digital Victoria:

- does not have full visibility of agencies' cybersecurity data
- cannot identify systemic issues or concerns across the sector.

This may affect Digital Victoria's ability to deliver the whole-of-government cyber operating model.

Using centralised SOCs

Under *Victoria's Cyber Strategy 2021* and its 2021–2023 mission delivery plans, Digital Victoria aims to set up centralised SOCs for agencies to use.

A SOC is an in-house or outsourced team of IT security professionals that monitors an agency's IT infrastructure 24/7 to detect and respond to cyber attacks.

The health sector set up its SOC in 2020. This is a good example of agencies detecting and responding to cybersecurity threats using a centralised solution.

Case study: The health sector's SOC helps health agencies monitor, detect and respond to cybersecurity threats.

In 2020 the former Department of Health and Human Services (now the Department of Health) helped set up a sector-wide SOC for health agencies.

The department oversees the provider who runs the SOC. It paid to set up the SOC and the first 3 years of ongoing management fees. The agencies that use it pay the ongoing management fees.

Over 120 health service providers, or 98 per cent, use the SOC. They receive sector-wide warnings and incident alerts to help them address threats.

The department holds monthly meetings with the SOC provider to discuss key performance and alert trends.

This arrangement helps the department monitor, identify and quickly respond to issues or threats that affect the entire sector.

Similarly, the Department of Premier and Cabinet and the former Department of Environment, Land, Water and Planning (now the Department of Energy, Environment and Climate Action) set up a water sector SOC in 2022.

As of March 2023, 17 water entities have planned to join the SOC. As of March 2023, 2 of these entities have finished the onboarding process. The rest are due to complete it by the end of 2024.

However, the current SOC arrangement does not provide services for protecting against cyber attacks. This duplicates effort because individual entities need to deliver this function independently.

It is often challenging for individual agencies to have the necessary resources and scale to establish cybersecurity teams with up-to-date knowledge and skills. This can expose agencies to high cybersecurity risks.

Appendices

Appendix A: Submissions and comments
Appendix B: Abbreviations, acronyms and glossary
Appendix C: Audit scope and method

Appendix A:
Submissions and comments

We have consulted with Cenitex, the Department of Education, the Department of Government Services, the Department of Health, the Department of Jobs, Skills, Industry and Regions, the Department of Premier and Cabinet, Grampians Health Horsham, Moorabool Shire Council, the Office of the Victorian Information Commissioner and South East Water and we considered their views when reaching our audit conclusions.

As required by the *Audit Act 1994*, we gave a draft copy of this report, or relevant extracts, to those agencies and asked for their submissions and comments.

Responsibility for the accuracy, fairness and balance of those comments rests solely with the agency head.

Responses received

Agency	Page
Cenitex	A–2
Department of Education	A–3
Department of Government Services	A–6
Department of Health	A–9
Department of Jobs, Skills, Industry and Regions	A–12
Department of Premier and Cabinet	A–15
Grampians Health Horsham	A–17
Moorabool Shire Council	A–19
Office of the Victorian Information Commissioner	A–21
South East Water	A–28

Response provided by the Chief Executive Officer, Cenitex

cenitex

Level 10, South Tower, 80 Collins St (PO Box 2750)
Melbourne, Victoria, 3000
ABN 56 375 109 796

25 July 2023

Mr Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Level 31, 35 Collins Street
Melbourne, Victoria, 3000

Dear Mr Greaves

Proposed Performance Audit Report Cybersecurity: cloud computing products

Thank you for your letter of 11 July 2023, enclosing your office's proposed performance audit report 'Cybersecurity: cloud computing products'.

The opportunity to respond to the draft report was appreciated and at that time I noted that the report acknowledges the outcome of Cenitex's long-term investment in cyber security and the competency of our people. It is pleasing that Cenitex has met the audit expectations in managing the shared Microsoft 365 tenancy.

The ability for Cenitex to provide our customers with reliable services to enable them to work from home during the pandemic without compromising information security was underpinned by focused attention and investment in cyber security.

Your team's engagement and open discussion of the environment and expectations has assisted my team further to clarify and differentiate roles and responsibilities in shared and managed service environments.

I am confident that your recommendations represent a significant opportunity to uplift the protection of public sector information and systems.

Cenitex have services that would assist the implementation of the recommendations in the report. We will seek to support agencies and departments through their implementation programs.

As part of our commitment to help Victorian Government organisations achieve their data protection objectives, Cenitex will continue to collaborate with our customers and create new partnerships.

I would like to take the opportunity once again to thank your team for their continued engagement with Cenitex.

Yours sincerely

[redacted]

Frances Cawthra
Chief Executive Officer

Classification: UNCLASSIFIED

cenitex

Response provided by the Secretary, Department of Education

Department of Education

Secretary

2 Treasury Place
East Melbourne Victoria 3002
Telephone +61 3 9637 2000

BRI23123772

Mr Andrew Greaves
Auditor-General
Victorian Auditor-General's Office

Dear Mr Greaves

Proposed report on Cybersecurity: Cloud Computing Products

Thank you for your letter of 11 July 2023 and the opportunity to comment on the proposed report for this audit. The department is committed to ensuring that cloud-based identity and device management controls are effective, in order to minimise cybersecurity risks.

The department has reviewed the proposed report and has attached an action plan to address the recommendations in the report.

Should you wish to discuss the department's response, please contact Shamiso Mtenje, Acting Executive Director, Integrity, Assurance and Executive Services Division on [redacted] or by email: [redacted].

Yours sincerely

[redacted]

Jenny Atta
Secretary
25/07/2023

Encl.: DE's action plan

DE action plan: Cyber Security – Cloud Computing Products

#	Recommendations:	Response	#	Action:	By (end of):
3	That audited agencies not using a security operation centre complete an independent risk assessment to inform whether they need a security operation centre to improve their cybersecurity and report the results of this assessment to their accountable officer and audit and risk committee. The risk assessment should: • identify the current gaps in their compliance and security posture as per the Victorian Government guidance and global standards • assess the capability and capacity of their cybersecurity team's knowledge, skills and resources.	Accept	3.1	The department accepts this recommendation, and has already identified the need for a Security Operation Centre / Managed Detection and Response service.	N/A – implemented
4	That audited agencies address the technical compliance control configuration weaknesses detailed in each agency's management letter.	Accept in principle	4.1	The department has undertaken a detailed risk assessment and will implement the technical compliance controls in relation to VPS and teaching service staff. A number of compliance controls in relation to, or dependent on, students using Multi-Factor cannot be implemented for students in government schools as they do not have access to mobile phones during school hours, in line with government policy.	March 2025
5	That audited agencies report the following to accountable risk owners at least quarterly: • their Microsoft Secure Score • a breakdown of controls completed by native solutions, third-party solutions and alternate mitigations • an adjusted Microsoft Secure Score that reflects the effectiveness of controls implemented by third-party solutions and alternative mitigations.	Accept	5.1	An adjusted Microsoft Secure Score will be added to the department's Cyber Security reporting to the accountable risk owner.	December 2023

DE action plan: Cyber Security – Cloud Computing Products

#	Recommendations:	Response	#	Action:	By (end of):
6	That audited agencies ensure accountable risk owners document their risk acceptance for controls marked as risk accepted, resolved via third-party solutions or alternative mitigations.	Accept	6.1	The department's current process for approving customisation of Microsoft 365 (M365) security configuration baselines will be expanded to include M365 control exception approvals by the accountable risk owners (i.e., risk accepted, third-party control and alternative mitigation).	February 2024
7	That audited agencies who use third-party services oversee and ensure that: • the services they buy from third-party providers meet their cyber security requirements • third-party service providers have implemented the controls they are responsible for • the implemented controls are effective.	Accept	7.1	The department accepts that it needs to oversee managed service providers to ensure they have implemented the controls the department requires. This will be formally incorporated into the department's managed service quarterly contract management arrangement for the M365 environment.	January 2024
			7.2	To ensure the implemented controls are effective, the department will annually request a certificate of compliance with *ISO 27001: Information Security Management* from all its third-party cybersecurity service providers.	September 2024

Response provided by the Secretary, Department of Government Services

Department of Government Services

Level 5
1 Macarthur Street
East Melbourne Victoria 3002
Telephone: (03) 9651 5111
dgs.vic.gov.au

Andrew Greaves
Auditor-General
Victorian Auditor-General Office
MELBOURNE VIC 3000

By email: [redacted]

Dear Mr Greaves

Response to the Victorian Auditor-General Office Proposed Report on Cybersecurity: Cloud Computing Products

The Department of Government Services (DGS) welcomes the opportunity to respond to the Proposed Report 'Cybersecurity: cloud computing products' (the Report).

Since its establishment on 1 January 2023, DGS has been focused on uplifting cyber security maturity across the Victorian Public Sector (VPS) to support the safe and reliable delivery of government services in line with the strategic vision and objectives of *Victoria's Cyber Strategy 2021-26*.

The 2023-24 State Budget provided DGS with an additional $34.7 million over two-years to further boost Victorian Government cyber defences, recognising the need to accelerate the protection of government systems and data against a rising cyber threat environment.

The additional funding will deliver:

- A new 24/7 Cyber Defence Centre to support the VPS in better identifying, blocking and responding to cyber-attacks – through enhanced intelligence sharing and expanded Security Operations Centre capability.
- Improved adoption of baseline cyber security controls, in particular the Australian Signals Directorate's Essential Eight, to reduce the risk of cyber-attacks on VPS organisations, to be delivered over a 12-month pilot program.
- Improved identification and protection of high-risk / high-value data systems and assets to ensure these systems and assets receive superior cyber security protections, to be delivered over a 12-month pilot program.
- The establishment of a new Cyber Security State Purchase Contract to improve the price and accessibility of commonly used cyber security products and services across the VPS, through shared purchasing arrangements.

While DGS plays a key central role in supporting improved public sector cyber maturity it does not own, nor have responsibility for, individual agencies' cyber security risk management. DGS will continue to support departments and agencies to establish and maintain a risk-based approach to cyber security, including supporting increased adoption of cloud technologies.

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

OFFICIAL

Response provided by the Secretary, Department of Government Services – *continued*

DGS was assigned two recommendations in the audit report. An action plan to address the two recommendations assigned to DGS is enclosed for your consideration.

Should you have any questions about the Department's feedback, please contact the Victorian Government Chief Information Security Officer, David Cullen by email at [redacted].

Yours sincerely

[redacted]

Jo de Morton
Secretary

24 / 07 / 2023

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

OFFICIAL

Department of Government Services action plan to address recommendations from Cybersecurity: Cloud Computing Products

No	VAGO recommendation	Agency acceptance level (e.g. accept/not accept)	Action plan	Completion date
1	Works with relevant agencies, including the Office of the Victorian Information Commissioner, to issue non-overlapping guidance that: • streamlines fragmented reporting requirements • balances security and productivity • does not create unintended consequences, such as multi-factor authentication fatigue. The guidance should mandate: • conditional access policy and device compliance policy configurations • additional technical control configurations consistent with the maturity model in this report • an issuer of device security configuration baselines. This mandate should apply to all classes of identities and devices used to access public sector resources, including but not limited to personal computers, mobile devices, guest users, ordinary users, privileged users, service accounts and non-human identities. Agencies should report their compliance against the issued guidance to their accountable risk owners and audit and risk committees at least annually.	Accept	DGS will work with the Office of the Victorian Information Commissioner and other cyber security stakeholders, including the Whole-of-Victorian-Government Cyber Security Leadership Group, to inform and support the development of new non-overlapping cyber security guidance for the public sector, to address the issues identified in this audit recommendation. DGS will work with OVIC to determine the appropriate body to issue the guidance, and the related timelines for release and implementation.	30 June 2024
2	Extends the cyber hubs and the security operation centres to: • maximise the number of Victorian public sector agencies • include protection services against cyber attacks	Accept- in-principle	DGS will address this recommendation through the new Cyber Defence Centre (CDC) program, funded in the 2023/24 State Budget. The CDC will extend security operations centre, cyber threat intelligence and incident operations capabilities to improve the protection of government systems and data against a rising cyber threat environment. The Cyber Hubs Program is not currently funded.	30 June 2024

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

OFFICIAL

Response provided by the Secretary, Department of Health

Secretary

Department of Health

50 Lonsdale Street
Melbourne Victoria 3000
Telephone: 1300 650 172
GPO Box 4057
Melbourne Victoria 3001
www.health.vic.gov.au
DX 210081

VAGO File No: 34165 21
DH File No: BAC-CO-38058

Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Via e-mail: [redacted]

Dear Mr Greaves

Thank you for providing my department with your proposed report for *the Cybersecurity: cloud computing products* performance audit.

My department has reviewed the proposed report, noting that there are seven recommendations in the report of which four recommendations are applicable to the Department of Health. I am pleased to include my department's actions in response to the recommendations as an attachment to this letter:

- Recommendation 4 - assess and develop implementation plan(s) to address the controls deficiencies detailed in the management letter using risk-based prioritisation.
- Recommendation 5 - implement a process to address the reporting requirements detailed in the recommendation regarding Microsoft Secure Score.
- Recommendation 6 - implement a process to ensure accountable risk owners document their risk acceptance for controls marked as risk accepted, resolved via third-party solutions or alternative mitigations.
- Recommendation 7 - the department will assess all cybersecurity services to ensure they are fit-for-purposes, for any found not fit-for-purpose, remediation plan(s) will be established.

I would like to have noted that whilst the performance audit focused on M365 cybersecurity controls, the department has other compensatory controls currently in place to provide stronger capabilities to protect the department's information from threats and risks.

All cybersecurity controls undergo regular assessment which includes continuously reviewing controls that are rated high in criticality and appropriate remedial actions are taken when required.

VICTORIA State Government

I would like to take this opportunity to thank your staff for working collaboratively with the Department of Health.

Yours sincerely

[redacted]

Professor Euan M Wallace AM
Secretary
21/07/2023

Department of Health action plan to address recommendations from Cybersecurity: Cloud Computing Products

No	VAGO recommendation	Agency acceptance level (e.g. accept/not accept)	Action plan	Completion date
Issue: Audited agencies' have ineffective Microsoft 365 cloud-based identity and device controls				
4	All audited agencies: Address the technical compliance control configuration weaknesses we detailed in each agency's management letter (see Section 2).	Accept	The department will assess and develop implementation plan(s) to address the controls deficiencies detailed in the management letter using risk-based prioritisation.	30 November 2023
5	All audited agencies: Report the following to accountable risk owners at least quarterly: • their Microsoft Secure Score • a breakdown of controls completed by native solutions, third-party solutions and alternative mitigations • an adjusted Microsoft Secure Score that reflects the effectiveness of controls implemented by third-party solutions and alternative mitigations (see Section 2).	Accept	A reporting process to address this recommendation will be implemented.	31 December 2023
6	Ensure accountable risk owners document their risk acceptance for controls marked as risk accepted, resolved via third-party solutions or alternative mitigations (see Section 2).	Accept	A risk acceptance process to address this recommendation will be implemented.	31 December 2023
Issue: Audited agencies insufficiently oversee cybersecurity services delivered by third-party providers				
7	All audited agencies who use third-party services: Oversee and ensure that: • the services they buy from third-party providers meet their cybersecurity requirements • third-party service providers have implemented the controls they are responsible for. • the implemented controls are effective (see Section 2).	Accept	The department will assess all cybersecurity services to ensure they are fit-for-purposes, for any found not fit-for-purpose, remediation plan(s) will be established.	30 June 2024

Response provided by the Secretary, Department of Jobs, Skills, Industry and Regions

OFFICIAL

Department of Jobs, Skills, Industry and Regions

GPO Box 4509
Melbourne ,Victoria 3001 Australia
Telephone: +61 3 9651 9999

Ref: CSEC-2-23-20455

Mr Andrew Greaves
Auditor General
Victorian Auditor General's Office
Level 31, 35 Collins Street
MELBOURNE VICTORIA 3000

Dear Mr Greaves

PROPOSED PERFORMANCE AUDIT REPORT – CYBERSECURITY: CLOUD COMPUTING

Thank you for your letter of 11 July 2023 regarding the Proposed Performance Audit Report - Cybersecurity: cloud computing products.

The Department of Jobs, Skills, Industry and Regions (the department) welcomes VAGO's recommendations and will continue to foster best practices and implement the remedial actions for strengthening its cybersecurity. The department has already outlined the corrective actions and time frames in the management letter which was shared with your team in May 2023. The department considers its response at management letter stage adequate and makes no further comments on the proposed report.

Finally, I appreciate the professional and diligent way this audit has been conducted. If you require further information, please contact Karan Gill, Chief Audit Officer on [redacted] or [redacted]

Yours sincerely

[redacted]

Tim Ada
Secretary

Date: 24/07/2023

<<Insert agency name>> action plan to address recommendations from Cybersecurity: Cloud Computing Products

No	VAGO recommendation	Agency acceptance level (e.g. accept/not accept)	Action plan	Completion date
1	Works with relevant agencies, including the Office of the Victorian Information Commissioner, to issue non-overlapping guidance that:	N/A - DGS	N/A	N/A
2	Extends the cyber hubs and the security operation centres to: • maximise the number of Victorian public sector agencies • include protection services against cyber attacks (see Section 3).	N/A – DGS	N/A	N/A
3	Complete an independent risk assessment to inform whether they need a security operation centre to improve their cybersecurity and report the results of this assessment to their accountable officer and audit and risk committee. The risk assessment should: • identify the current gaps in their compliance and security posture as per the Victorian Government guidance and global standards • assess the capability and capacity of their cybersecurity team's knowledge, skills and resources (see Section 3).	N/A – DJSIR utilise Cenitex SOC	N/A	N/A
4	Address the technical compliance control configuration weaknesses we detailed in each agency's management letter	Accepted	Please see Management letter (May) for detailed response	As per Management letter
5	Report the following to accountable risk owners at least quarterly: • their Microsoft Secure Score • a breakdown of controls completed by native solutions, third-party solutions and alternative mitigations • an adjusted Microsoft Secure Score that reflects the effectiveness of controls implemented by third-party solutions and alternative mitigations (see Section 2)	Accepted	DJSIR will work with Cenitex to gain access to Microsoft Secure scores quarterly and report to accountable risk owners	30 April 2024

6	Ensure accountable risk owners document their risk acceptance for controls marked as risk accepted, resolved via third-party solutions or alternative mitigations (see Section 2).	Accepted	DJSIR has an established risk acceptance process, this will now extend to risk relating to Microsoft secure scores once this process is established with Cenitex	30 April 2024
7	Oversee and ensure that: • the services they buy from third-party providers meet their cybersecurity requirements • third-party service providers have implemented the controls they are responsible for. • the implemented controls are effective (see Section 2).	Accepted	DJSIR will work with third party providers to ensure that security controls have been implemented.	30 June 2024

Response provided by the Secretary, Department of Premier and Cabinet

Department of
Premier and Cabinet

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

BSEC-230700611

Mr Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Level 31, 35 Collins Street
MELBOURNE VIC 3000

Dear Auditor-General

I am writing in response to your letter dated 11 July 2023 enclosing the proposed Performance Audit Report on Cybersecurity: cloud computing products.

The Department of Premier and Cabinet (DPC) attaches its action plan to acquit the proposed performance audit recommendations in the Audit Report. DPC has carefully considered the report and has accepted all applicable recommendations.

Thank you for the opportunity to respond to the recommendations and findings of the Performance Audit Report.

Yours sincerely

[redacted]

Jeremi Moule
Secretary
28 / 07 / 2023

Encl.

VICTORIA State Government

Response provided by the Secretary, Department of Premier and Cabinet – *continued*

Department of Premier and Cabinet action plan to address recommendations from the Cybersecurity: Cloud Computing Products Victorian Auditor-General's Office performance audit

No	VAGO recommendation	Agency acceptance level (e.g. accept/not accept)	Action plan	Completion date
1	DGS-specific.	N/A.	N/A	N/A.
2	DGS-specific.	N/A	N/A	N/A
3	Complete an independent risk assessment to inform whether they need a security operation centre to improve their cybersecurity and report the results of this assessment to their accountable officer and audit and risk committee. The risk assessment should: • identify the current gaps in their compliance and security posture as per the Victorian Government guidance and global standards • assess the capability and capacity of their cybersecurity team's knowledge, skills and resources.	N/A – DPC currently utilise the Cenitex Security Operations Centre.	N/A	Complete
4	Address the technical compliance control configuration weaknesses we detailed in each agency's management letter (see Section 2).	Accept	DPC will work with the CENITEX Cyber Security Customer Group and CISO to remediate configuration weaknesses.	31/12/24.
5	Report the following to accountable risk owners at least quarterly: • their Microsoft Secure Score • a breakdown of controls completed by native solutions, third-party solutions and alternative mitigations • an adjusted Microsoft Secure Score that reflects the effectiveness of controls implemented by third-party solutions and alternative mitigations (see Section 2).	Accept	DPC will provide their Microsoft Secure Score as part of its quarterly internal control update. DPC will also review the Microsoft Secure score to ensure it reflects the effectiveness of controls implemented by third-party solutions.	31/12/23.
6	Ensure accountable risk owners document their risk acceptance for controls marked as risk accepted, resolved via third-party solutions or alternative mitigations (see Section 2).	Accept	DPC will organise for accountable risk owners to attest to risks that have been accepted, resolved via third party-solutions or alternative mitigations and determine the frequency of the attestation.	1/7/24
7	Oversee and ensure that: • the services they buy from third-party providers meet their cybersecurity requirements • third-party service providers have implemented the controls they are responsible for. • the implemented controls are effective (see Section 2).	Accept	DPC will implement a process to ensure vendors display adequate cyber security controls during the procurement process and ensure contract management plans include the review of these controls throughout the life of the contract.	31/12/24.

Response provided by the Chair, Grampians Health Horsham

Grampians Health

Ballarat Campus
Drummond Street North
Ballarat, Victoria 3350
PO Box 577
Ballarat, Victoria 3350

25 July 2023

Andrew Greaves
Auditor General
Victorian Audit General's Office
Level 31, 35 Collins Street
Melbourne, Victoria 3000

Dear Auditor General,

RE: Cybersecurity: Cloud Computing Products

Thank you for your letter dated 11 July 2023 and the opportunity to respond to the proposed report.

Please find enclosed Grampians Health's action plan to address the recommendations of the proposed report as per the Victorian Auditor General's Office (VAGO) template provided.

Cybersecurity threats in Victoria as your office has identified are a real and growing threat.

Grampians Health accepts the 7 recommendations to address the 3 key findings; noting recommendations numbered 3 - 7 pertain to the audited agencies.

Grampians Health is committed to continuously strengthening our cybersecurity posture. Given the sensitivities of this audit, Grampians Health will monitor detailed progress through our internal Audit and Risk Committee.

Should you have any further queries or require further information, please contact Dale Fraser, Chief Executive Officer or Kate Nolan, Chief Information Officer.

Yours faithfully,

Bill Brown
Chair
Grampians Health Board
cc: Dale Fraser, Kate Nolan

Grampians Health Ballarat | Grampians Health Dimboola | Grampians Health Edenhope | Grampians Health Horsham | Grampians Health Stawell

Response provided by the Chair, Grampians Health Horsham – *continued*

Grampians Health Horsham action plan to address recommendations from Cybersecurity: Cloud Computing Products

No	VAGO recommendation	Agency acceptance level (e.g. accept/not accept)	Action plan	Completion date
1	*DGS specific*	Noted	N/A	
2	*DGS specific*	Noted	N/A	
3	*Non-Security Operations Centre (SOC) agencies*	Noted	Grampians Health will continue with established Security Operations Centre (SOC).	Completed
4	Address technical compliance control configuration weaknesses	Accept	Grampians Health accept the recommendations as per returned management comments. Management of actions will occur through the Audit and Risk Committee.	30/11/2024
5	Quarterly reporting to accountable risk owners	Accept	Grampians Health accept the recommendation, and will build into the cybersecurity operational report.	29/02/2024
6	Risk owners document risk acceptance / resolution / mitigation	Accept	Grampians Health accept the recommendation and will capture risk acceptance of implemented controls and mitigations.	30/04/2024
7	Oversight of third-party service providers security requirements	Accept	Grampians Health accept the recommendation, and we will establish processes to regularly review controls implemented / maintained by third-party services.	29/03/2024

Response provided by the General Manager Customer Care and Advocacy, Moorabool Shire Council

Moorabool
Shire Council

25 July 2023

Andrew Greaves
Auditor General

Dear Andrew

Re: Proposed Performance Audit Report - Cybersecurity: cloud computing products

Thank you for your recent correspondence regarding Moorabool Shire Council's involvement with the Audit.

Please find included Moorabool's Action Plan in response to the Audit recommendations for your records.

With regards to Recommendation 1 (that Department of Government Services Works with relevant agencies to issue non-overlapping guidance etc), Moorabool would like to note that DGS implementation of mandated guidance runs the risk of being significantly onerous for local government (particularly smaller Councils) unless associated overheads to implementation are acknowledged and funded by State Government, or that there is flexibility in the mandated guidance (similar to the existing Essential 8 model).

With regards to Recommendation 2 (that Department of Government Services extends cyber hubs and the security operation centres), Moorabool would like to advocate for any extended services to be delivered at no additional cost to public & (particularly) local government agencies. At present there is no cost for federal and state related cyber services, however expansion of cyber services could potentially see on-selling between agencies. This would once again be significantly difficult for smaller Councils.

Yours sincerely

[redacted]

Caroline Buisson
General Manager Customer Care and Advocacy

Mail PO Box 18 Ballan Vic 3342
Ballan 15 Stead St Ballan
Bacchus Marsh 215 Main St Bacchus Marsh
Darley 182 Halletts Way Darley

P (03) 5366 7100
E info@moorabool.vic.gov.au
W www.moorabool.vic.gov.au
ABN 293 5275 4296

facebook.com/mooraboolshirecouncil
twitter.com/mooraboolshire

Response provided by the General Manager Customer Care and Advocacy, Moorabool Shire Council – *continued*

Moorabool Shire Council action plan to address recommendations from Cybersecurity: Cloud Computing Products

No	VAGO recommendation	Agency acceptance level (e.g. accept/not accept)	Action plan	Completion date
1	Department of Government Services Works with relevant agencies, including the Office of the Victorian Information Commissioner, to issue non-overlapping guidance…	NA	NA	NA
2	Department of Government Services Extends the cyber hubs and the security operation centres	NA	NA	NA
3	All audited agencies that are not using a security operation centre Complete an independent risk assessment to inform whether they need a security operation centre to improve their cybersecurity and report the results of this assessment to their accountable officer and audit and risk committee	NA	NA	We have a SOC
4	Address the technical compliance control configuration weaknesses we detailed in each agency's management letter	Accept	We will report the VAGO findings to our ARC with recommendations and remediations	All actions to be completed by June 2025
5	Report the following to accountable risk owners at least quarterly: • their Microsoft Secure Score • a breakdown of controls completed by native solutions, third-party solutions and alternative mitigations • an adjusted Microsoft Secure Score that reflects the effectiveness of controls implemented by third-party solutions and alternative mitigations	NA	NA	This is already done
6	Ensure accountable risk owners document their risk acceptance for controls marked as risk accepted, resolved via third-party solutions or alternative mitigations	Accept	We will present the results of the VAGO audit at the November ARC meeting	Dec 2023
7	Oversee and ensure that: • the services they buy from third-party providers meet their cybersecurity requirements • third-party service providers have implemented the controls they are responsible for. • the implemented controls are effective	Accept	We currently have a process to ensure our security requirements from 3rd party vendors. We recently implemented a tool (UpGuard) that facilitates management of these requirements. We will implement UpGuard capability across our key 3rd party providers.	June 2024

Response provided by the Information Commissioner, Office of the Victorian Information Commissioner

OFFICIAL

Office of the Victorian Information Commissioner

Phone: 1300 00 6842
Email: enquiries@ovic.vic.gov.au
PO Box 24274
Melbourne Victoria 3001

28 July 2023

Mr Andrew Greaves
Auditor-General
Victorian Auditor-General's Office

By email only: [redacted]

Dear Mr Greaves,

Cybersecurity: Cloud Computing Products Audit

Thank you for your letter of 11 July 2023 and the opportunity to comment on the Proposed Report for this audit.

OVIC is in the process of transitioning to the M365 environment and welcomes the findings provided by the VAGO team. The control weaknesses identified have been reviewed in the context of OVIC's current work program and where appropriate actioned utilising our risk management framework.

We note the audit recommends OVIC work with Department of Government Services to issue non-overlapping guidance including the issuing of mandatory technical controls. Consistent with the Victorian protective Data Security Framework and Standards (as endorsed by government and in force through legislation), organisations are required to employ a risk-based approach to enhance information security capability and maturity, with existing risk management principles and guidelines. While supportive of work that offers new controls to deal with threats, OVIC is concerned that a shift to "compliance" thinking will undercut the extensive work that has been done to spur better risk assessments within agencies. We appreciate your comment that adoption or rejection of M365 controls needs to be assessed in the context of properly documented risk assessments.

OVIC aims to conduct another review of the Victorian Protective Data Security Standards (**VPDSS**) and their elements should Government provide funding in the future. In the interim, consistent with current legislation and appropriate consultation, OVIC will continue to evolve the Framework and Standards to safeguard information assets and systems in a manner that is proportionate to threats and supportive of business outcomes.

Response provided by the Information Commissioner, Office of the Victorian Information Commissioner – *continued*

Finally, we thank you for including in your report the caveat that it relates to M365 cloud services only.

Yours sincerely

Sven Bluemmel
Information Commissioner

Encl. Office of the Victorian Information Commissioner action plan to address recommendations from Cybersecurity: Cloud Computing Products

Response provided by the Information Commissioner, Office of the Victorian Information Commissioner – *continued*

OFFICIAL

Office of the Victorian Information Commissioner action plan to address recommendations from Cybersecurity: Cloud Computing Products

No.	Responsible	VAGO recommendation	Agency acceptance level (e.g. accept/not accept)	Action plan	Completion date
Issue: The public sector lacks a coordinated approach to address cybersecurity risks					
1	Department of Government Services and the Office of the Victorian Information Commissioner	Work together, in consultation with other relevant agencies to issue non-overlapping guidance that: • streamlines fragmented reporting requirements • balances security and productivity • does not create unintended consequences, such as multi-factor authentication fatigue. The guidance should mandate: • conditional access policy and device compliance policy configurations • additional technical control configurations consistent with the maturity model in this report • an issuer of device security configuration baselines. This mandate should apply to all classes of identities and devices used to access public sector resources, including but not limited to personal computers,	Accept with qualification	OVIC will work with DGS to deliver guidance material with recommended rather than mandatory controls, in line with the organisations risk assessments under the VPDSS.	Ongoing

OFFICIAL

Response provided by the Information Commissioner, Office of the Victorian Information Commissioner – *continued*

No.	Responsible	VAGO recommendation	Agency acceptance level (e.g. accept/not accept)	Action plan	Completion date
		mobile devices, guest users, ordinary users, privileged users, service accounts and non-human identities. Agencies should report their compliance against the issued guidance to their accountable risk owners and audit and risk committees at least annually (see Section 3).			
2.	Department of Government Services	Extends the cyber hubs and the security operation centres to: • maximise the number of Victorian public sector agencies • include protection services against cyber attacks (see Section 3).	N/A	N/A	
3.	All audited agencies that are not using a security operation centre	Complete an independent (internal or external) risk assessment to inform whether they need a security operation centre to improve their cybersecurity and report the results of this assessment to their accountable officer and audit and risk committee. The risk assessment should: • identify the current gaps in their compliance and security posture as per the Victorian Government guidance and global standards	Accept	This will be included in OVIC's current program of work.	2024

Response provided by the Information Commissioner, Office of the Victorian Information Commissioner – *continued*

No.	Responsible	VAGO recommendation	Agency acceptance level (e.g. accept/not accept)	Action plan	Completion date
		• assess the capability and capacity of their cybersecurity team's knowledge, skills and resources (see Section 3).			
Issue: Audited agencies' have ineffective Microsoft 365 cloud-based identity and device controls					
4.	All audited agencies	Address the technical compliance control configuration weaknesses we detailed in each agency's management letter (see Section 2).	Accept	Detailed action plan provided to VAGO	Detailed timeframes provided to VAGO
5.	All audited agencies	Report the following to accountable risk owners at least quarterly: • their Microsoft Secure Score • a breakdown of controls completed by native solutions, third-party solutions and alternative mitigations • an adjusted Microsoft Secure Score that reflects the effectiveness of controls implemented by third-party solutions and alternative mitigations (see Section 2).	Accept	OVIC are currently reporting their security score to multiple governance committees and address any control gaps in line with OVIC's risk management framework. As the Microsoft 365 environment is constantly updated with enhanced security features, this will be an ongoing program of work.	Ongoing

Response provided by the Information Commissioner, Office of the Victorian Information Commissioner – *continued*

No.	Responsible	VAGO recommendation	Agency acceptance level (e.g. accept/not accept)	Action plan	Completion date
6.	All audited agencies	Ensure accountable risk owners document their risk acceptance for controls marked as risk accepted, resolved via third-party solutions or alternative mitigations (see Section 2).	Accept	As OVIC migrate to the Microsoft 365 environment, risks are identified and managed by the accountable risk owners in line with OVIC's risk management framework. As the Microsoft 365 environment is constantly updated with enhanced security features, this will be an ongoing program of work. There will be no end date.	Ongoing
Issue: Audited agencies insufficiently oversee cybersecurity services delivered by third-party providers					
7.	All audited agencies who use third-party services	Oversee and ensure that: • the services they buy from third-party providers meet their cybersecurity requirements • third-party service providers have implemented the controls they are responsible for. • the implemented controls are effective (see Section 2).	Accept	OVIC have assessed their Microsoft 365 environment against the • Australian Government Digital Transformation Agency Blueprint designed to secure Microsoft 365 at the PROTECTED Level. • M365 Secure Score • Australian Government Information Security Manual (ISM) suite of controls.	Ongoing

Response provided by the Information Commissioner, Office of the Victorian Information Commissioner – *continued*

OFFICIAL

No.	Responsible	VAGO recommendation	Agency acceptance level (e.g. accept/not accept)	Action plan	Completion date
				As these suites of controls are established under a risk-based approach, OVIC will continue to address any control gaps in line with OVIC's risk management framework.	

OFFICIAL

Response provided by the Chair, South East Water

South East Water

Healthy Water.
For Life.

WatersEdge
101 Wells Street
Frankston VIC 3199

P.O. Box 2268
Seaford VIC 3198
Australia

t +61 39552 3000

southeastwater.com.au

25 July 2023

Andrew Greaves
Auditor General
Victorian Auditor-General Office
Level 31/35 Collins Street
Melbourne 3000

Dear Mr Greaves

Proposed Performance Audit Report – Cybersecurity: cloud computing products

We would like to take this opportunity to thank the Victorian Auditor-General Office (VAGO) for undertaking this audit and including South East Water (SEW). The team at South East Water has found this audit to be extremely valuable for our cyber security program.

Please find our response to the audit findings, noting that we accept all recommendations made by VAGO.

No	VAGO recommendation	Agency acceptance level (e.g., accept/not accept)	Action plan	Completion date
1	The public sector lacks a coordinated approach to address cybersecurity risks.	Not applicable as finding is focused on the Department of Government Services		
2	The public sector lacks a coordinated approach to address cybersecurity risks.	Not applicable as finding is focused on the Department of Government Services		
3	All audited agencies that are not using a security operation centre.	Not applicable as SEW has implemented the Victorian Government recommended security operation centre.		
4	Address the technical compliance control configuration weaknesses we detailed in each agency's management letter.	Accepted	To implement the recommendations as detailed in the management letter	Various dates as per management letter response
5	Report Microsoft security score at least quarterly.	Accepted	Microsoft security score to be included in the quarterly security dashboard	Implemented
6	Ensure accountable risk owners document their risk acceptance for controls.	Accepted	Configuration changes will be captured in SEW risk register	On going
7	Audited agencies insufficiently oversee cybersecurity services	Not applicable as SEW manages our information		

South East Water Corporation
ABN 89 066 902 547

South East Water

No	VAGO recommendation	Agency acceptance level (e.g., accept/not accept)	Action plan	Completion date
	delivered by third-party providers.	technology environments internally.		

Yours Sincerely

[redacted]

Ms Lucia Cade
Chair, South East Water

South East Water Corporation
ABN 89 066 902 547

Appendix B: Abbreviations, acronyms and glossary

Abbreviations

We use the following abbreviations in this report:

Abbreviation	
secure score	Microsoft Secure Score

Acronyms

We use the following acronyms in this report:

Acronym	
BYOD	bring your own device
CIEM	cloud infrastructure entitlement management
CIS	Center for Internet Security
DISA	Defence Information Systems Agency
EDR	endpoint detection and response
EMM	enterprise mobility management
EPP	Endpoint Protection Platform
IAM	identity and access management
IT	information technology
MAM	mobile application management
MCSB	Microsoft cloud security benchmark
MDM	Mobile Device Management
MFA	multi-factor authentication
MTD	Mobile Threat Defence
NGAV	Next Generation Anti-virus
SIEM	security information and event management
SOAR	Security Orchestration, Automation, and Response
SOC	security operation centre
UEM	unified endpoint management
UES	unified endpoint security
VAGO	Victorian Auditor-General's Office
XDR	extended detection and response

Glossary

This glossary includes an explanation of the types of engagements we perform:

Term	
Reasonable assurance	We achieve reasonable assurance by obtaining and verifying direct evidence from a variety of internal and external sources about an agency's performance. This enables us to express an opinion or draw a conclusion against an audit objective with a high level of assurance. We call these audit engagements. See our assurance services fact sheet for more information.
Limited assurance	We obtain less assurance when we rely primarily on an agency's representations and other evidence generated by that agency. However, we aim to have enough confidence in our conclusion for it to be meaningful. We call these types of engagements assurance reviews and typically express our opinions in negative terms. For example, that nothing has come to our attention to indicate there is a problem. See our assurance services fact sheet for more information.
The cloud	The cloud is when a service provider supplies software, data storage and other services over the internet. The cloud is more economical, effective and efficient compared to traditional computing, which relies on in house servers and databases.
Compliance policy	A compliance policy is a set of rules that a device must comply with. For example, an agency may require devices to have antivirus software.
Conditional access policies	Agencies can implement conditional access policies to require a user to complete an action if they want to access their networks.
Cybersecurity solution	Modern cybersecurity solutions use technology such as threat and artificial intelligence to analyse user behaviours and other signals. These solutions can be used to detect and respond to threats. A native cybersecurity solution is one from the cybersecurity platform provider, such as Microsoft.
Managed service arrangement	Under a managed service arrangement, the agency determines and oversees the controls. The service provider is responsible for implementing them.
MFA	MFA is a control that requires users to verify their identity using at least 2 methods before they can access an agency's systems or documents.
Microsoft 365 tenancy	A Microsoft 365 tenancy is a dedicated environment within the Microsoft 365 cloud. It provides a range of services from Microsoft. When an agency buys a Microsoft 365 subscription, it is allocated to a tenancy. Agencies can share a tenancy.
Passwordless authentication	Passwordless authentication lets a user access an application or IT system without entering a password. Instead, the user may log in with passwordless technology, such as biometrics. This reduces the risk of people relying on remembering passwords to access systems.
Privileged access management	Agencies can give some users access to more functions than standard users, such as accessing, modifying or deleting sensitive information as well as making changes to servers, devices and user accounts.
Security configuration baseline	A security configuration baseline is the recommended settings that an agency can use to set up its devices.
Shared service arrangement	Under a shared service arrangement, the service provider determines and implements controls. An agency needs to assess if the controls meet its requirements before entering the engagement.

Term	
The zero trust model's 6 pillars	Identities, devices, applications, data, infrastructure and networks are 6 foundational elements, or pillars, that make up modern IT operations. The zero trust model is a high-level strategy. It assumes that users, devices and services attempting to access resources, even from inside the network, cannot automatically be trusted.

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.

Auditor-General's reports tabled during 2023–24

Report title	Tabled
Cybersecurity: Cloud Computing Products (2023–24: 1)	August 2023

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

Our role and contact details

The Auditor-General's role

For information about the Auditor-General's role and VAGO's work, please see our online fact sheet About VAGO.

Our assurance services

Our online fact sheet Our assurance services details the nature and levels of assurance that we provide to Parliament and public sector agencies through our work program.

Contact details

Victorian Auditor-General's Office
Level 31, 35 Collins Street
Melbourne Vic 3000
AUSTRALIA

Phone +61 3 8601 7000
Email enquiries@audit.vic.gov.au