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

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