VAGO
Victorian Auditor-General's Office

Cybersecurity of IT Servers

October 2025

Independent assurance report to Parliament
2025–26: 6

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 978-1-921650-16-1

VAGO
Victorian Auditor-General's Office

Cybersecurity of IT Servers

Independent assurance report to Parliament
Published by order, or under the authority,
of the Parliament of Victoria
October 2025

VAGO
Victorian Auditor-General's Office

The Hon Shaun Leane MLC
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 of IT Servers*.

Yours faithfully

Andrew Greaves
Auditor-General
29 October 2025

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

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

Why we did this audit

In 2023, 9 out of 10 Victorian Government organisations experienced a cyber incident. A successful cyber attack can lead to confidential or sensitive information being leaked and can disrupt communication networks and critical infrastructure.

Agencies use IT servers (servers) to store, process and share information to support service delivery. Servers are central to IT systems because they let multiple users access valuable information and functions. If servers are unidentified, do not have mature security controls or have out-of-date operating systems, this can make it easier to gain unauthorised access to information and systems.

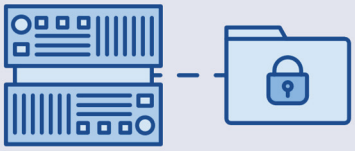
Effective cybersecurity measures help protect servers against cyber threats. This audit assessed if government agencies:

- know what servers they have
- implement mature security controls to their servers
- check that the controls they apply work as intended.

This is our second report examining cybersecurity in the Victorian Public Service. Our first report in 2023 found that audited agencies could improve their cloud-based identity management and device management controls.

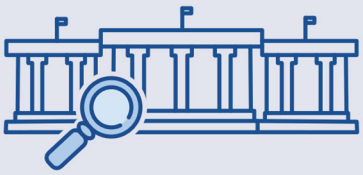
Key background information

Agencies use **servers** to store, process and share **information** to support service delivery



This information can be **personal** or **sensitive**

We audited the technical security controls of servers for **10 government departments** and **Cenitex**



We focused on

5 key elements

of **server security**

Source: VAGO.

What we concluded

Each agency can do more to improve its server security.

A complete and accurate server inventory is a critical foundation for effective cybersecurity. No audited agency has a complete and accurate inventory of their servers. Without this, agencies cannot reliably apply, manage or monitor the technical security controls needed to protect their servers.

All agencies have outdated operating systems and some servers that lack mature technical security controls. These gaps expose agencies to cyber threats and increase the risk of successful cyber attacks.

We made 2 recommendations for all agencies to improve tracking of their servers and to strengthen the technical security controls applied to them. We made one recommendation for the Department of Government Services to issue guidance on expectations for server security.

1.
Our key findings

What we examined

Our audit followed 2 lines of inquiry:

1. Do agencies track all their servers and apply foundational security controls to them?
2. Do agencies monitor their server security and strengthen it in response to threats?

To answer these questions, we examined:

- server inventory information
- technical security controls applied by agencies to their IT servers against the Microsoft cloud security benchmark (MCSB)
- threat and vulnerability monitoring and reporting activities.

We gathered information on technical security controls applied by agencies via a survey and interviews.

Background information

Why server security is important

Victorian Government agencies use servers to store, process and share information and programs to support service delivery and administration. Servers can contain personal or sensitive information about public sector employees or users of public services.

A single vulnerable server can be a pathway for cyber attackers to compromise an IT system or gain unauthorised access to information.

Applying effective cybersecurity measures to IT infrastructure, including servers, is essential to reducing the risk of cybersecurity incidents.

Server

A physical (hardware) or virtual (software) computer that provides services over a digital network to other computers. For example, servers run operating systems and applications, host databases and store information.

Incident

An event that actually or potentially threatens the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits. An incident can also be a violation or imminent threat of violation of security policies, security procedures or acceptable-use policies.

Vulnerability

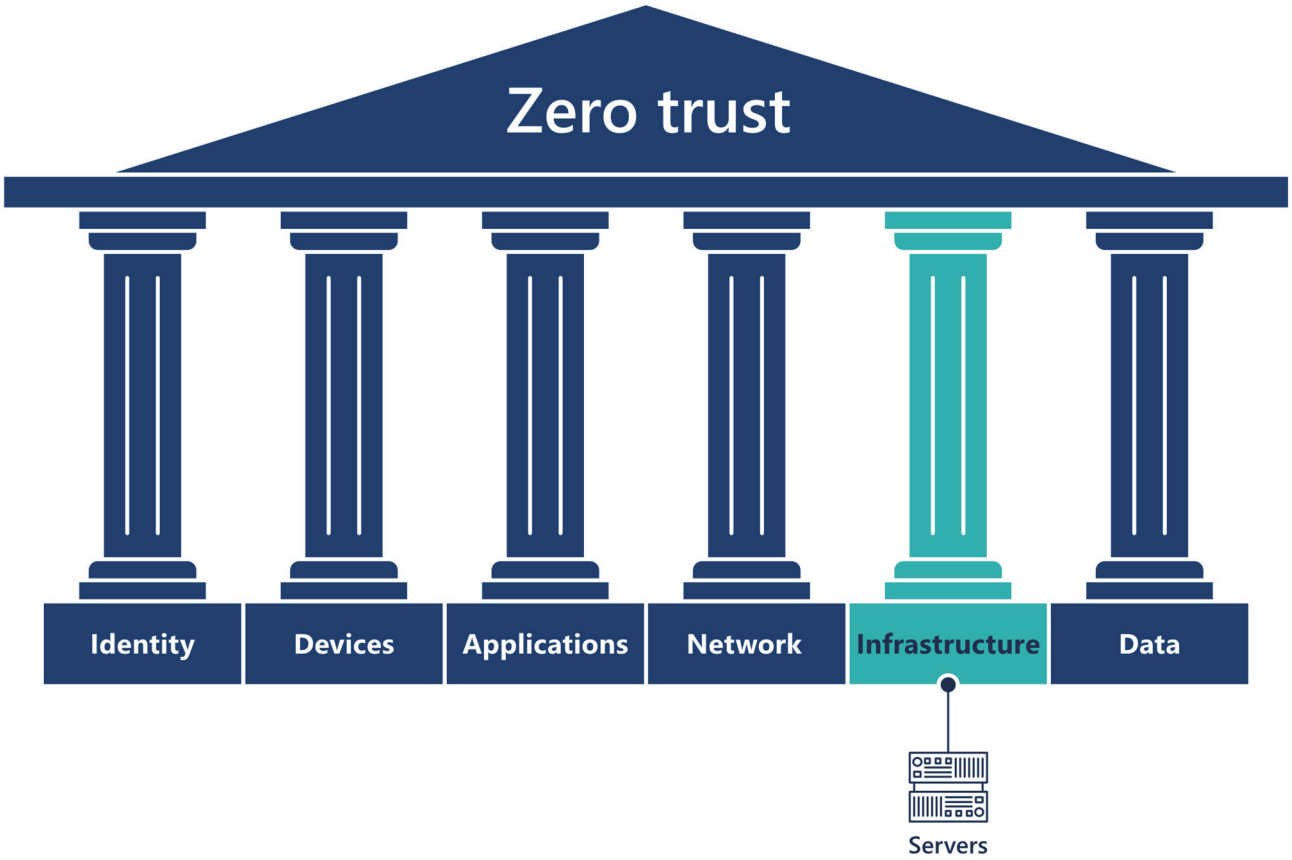
A weakness in an information system, its security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

The zero-trust model

Zero trust is a security model based on the position of not trusting anything inside or outside an agency's network. Infrastructure is one of the 6 pillars of zero trust, and servers are part of the infrastructure pillar.

Server security must work with protections across all other pillars of the zero-trust model to optimise cybersecurity.

Figure 1: The 6 pillars of zero trust



Source: VAGO, based on information from Microsoft.

Cybersecurity
Cybersecurity is the practice of protecting the confidentiality, integrity and availability of computer systems and information.

Cybersecurity standards, strategies and frameworks

The Victorian Government provides agencies with various standards, strategies and frameworks about cybersecurity.

In ...	the Victorian Government provides information on ...
Victoria's Cyber Strategy 2021	its cyber agenda and defines its long-term objectives.
the *Victorian Government Digital Strategy 2021–26*	its vision for digital transformation, including: • delivering more accessible public services • improving the digital capacity and capabilities of the public sector.
the *Victorian Government IT Asset Management Guidance*	• maintaining visibility of IT infrastructure • ensuring IT asset registers hold complete and correct data.
the *Victorian Protective Data Security Standards*	• managing all information and communications technology (ICT) assets throughout their lifecycle • maintaining a secure environment by protecting the organisation's public sector information through ICT security controls.
the *Asset Management Accountability Framework*	asset management, including information management, over the asset lifecycle.
the *Victorian Government Cloud Security Guidance*	making informed, risk-based decisions about using cloud services.

Difference between ICT and IT

ICT is a broader term that includes IT and other communications technologies, such as telecommunications.

IT is a subset of ICT that focuses on using systems for storing, retrieving and sending information.

Roles and responsibilities

Agencies are accountable for the cybersecurity of their servers. Standard 11 in the *Victorian Protective Data Security Standards* requires agencies to establish, implement and maintain ICT security controls.

Some agencies manage their own servers, and some choose to engage a service provider to manage all or part of their server inventory and security.

The *Victorian Government Cloud Security Guidance* outlines that agencies:

- are responsible for understanding if the security capability provided by a third party is appropriate to the risk within their IT environments
- should determine if any further controls are required.

Even if an agency outsources its server security, it is responsible for:

- ensuring the controls implemented are appropriate for its risk profile and appetite
- ensuring security controls are effective.

Department of Government Services

The Department of Government Services (DGS) is the agency responsible for cybersecurity across government, specifically through its cybersecurity unit.

The cybersecurity unit supports Victorian government agencies with:

- expert cybersecurity threat advice
- strategic guidance
- risk analysis and assurance.

The cybersecurity unit also implements the Mission Delivery Plans under *Victoria's Cyber Strategy 2021*.

Cenitex

Cenitex is a state-owned enterprise that delivers ICT services to Victorian Government departments and agencies. Cenitex manages a suite of IT products. It is not mandatory for government agencies to use Cenitex's services, though many do. Some agencies use other third-party service providers.

Technical security controls

The technical security measures that agencies use to protect their servers, such as configurations, settings and policies.

How we have reported findings for individual agencies

We audited the cybersecurity measures applied to servers of Victoria's 10 government departments and Cenitex. Due to the sensitive nature of the security weaknesses we found, our report does not attribute findings to particular agencies. Each agency has received a separate report outlining the weaknesses we found in their technical security controls.

The Department of Health (DH) is represented across 2 entities in our analysis, reflecting the structure of its server environment:

- Health Technology Services is a business unit in DH that provides ICT services to health service providers. In this report, Health Technology Services is treated as a separate entity.
- Other business units of DH share a server platform with the Department of Families, Fairness and Housing. This shared environment is treated as a single entity for the purposes of our report.

What we found

This section focuses on our key findings, which fall into 2 areas:

1. No agency has a complete and accurate server inventory.
2. All agencies can improve the maturity of technical security controls applied to their known servers.

The full list of our recommendations, including agency responses, is at the end of this section.

Consultation with agencies

When reaching our conclusions, we consulted with the audited agencies and considered their views.

You can read their full responses in Appendix A.

Key finding 1: No agency has a complete and accurate server inventory

No agency provided us with a complete and accurate server inventory. Maintaining a complete and accurate server inventory, including each server's key attributes, is a foundation of effective cybersecurity. Without this, agencies cannot make sure appropriate controls are in place.

Automated asset discovery tools are not set up to capture all servers

Automated asset discovery tools can provide agencies with visibility over:

- what servers they have
- where their servers are located
- how their servers are being used.

The *Victorian Government IT Asset Management Guidance* and the MCSB point to using automated asset discovery tools as best practice when managing server assets.

Six agencies use passive or active automated asset discovery tools to identify the servers in their network. However, none of these agencies had their automated asset discovery tools set up to cover their entire server environment. This increases the risk that agencies' inventories are incomplete or outdated.

Not all agencies reconcile server information

Agencies can compare and reconcile different information sources to verify their server inventory.

Three agencies reconcile their server inventory across all their server environments. These agencies use processes such as completing an audit of their server inventory and manual verification of server entries.

Server reconciliations are not, however, considered best practice on their own. Best practice typically involves automated asset discovery.

All agencies have server information that is inaccurate or incomplete

We asked all agencies to provide us with an inventory for all their on-premises and infrastructure as a service (IaaS) servers.

Server inventories for all agencies contained incomplete information, such as missing:

- operating system version names or numbers
- host names
- location information.

Eight agencies' inventories included duplicated server records. This points to weaknesses in how agencies track their server environments.

Infrastructure as a service (IaaS)

A cloud-computing model that delivers on-demand servers, storage and networking. This allows businesses to rent resources, adjust to changing demands for resources and reduce hardware costs.

Addressing this finding

To address this finding, we have made one recommendation to all agencies to improve tracking and accountability for their servers.

Key finding 2: All agencies can improve the maturity of technical security controls applied to their known servers

All agencies have applied technical security controls to their servers. However, the maturity of these controls is low when compared with industry benchmarks.

All agencies are running servers with outdated operating systems. This provides them with a lower level of protection than more recent systems.

Agencies' technical security controls have low maturity based on industry benchmarks

We considered the maturity of the technical security controls applied by agencies across key elements of server security, including operating systems, security baselines and backup and monitoring. We based our analysis on the MCSB.

Based on this benchmark, we assessed that all agencies have low maturity in terms of the technical security controls applied to their known servers. Some agencies had a higher level of maturity for specific controls, demonstrating some elements of better practice for their known servers.

All agencies have servers with operating systems that are not receiving mainstream support

Most servers are running operating systems that are not receiving mainstream support.

We asked agencies to provide us with their server inventory information, including information on server operating systems. Twenty-five per cent of servers reported by agencies have operating systems that are unsupported and not receiving automatic security updates. A further 11 per cent of server entries reported by agencies had unknown operating systems.

All agencies have unsupported operating systems running on some servers. This makes them more vulnerable to cyber attacks.

All agencies monitor their servers for threats and vulnerabilities. However, agencies cannot be sure that their monitoring activities are fully effective until they address identified gaps in their server inventories and technical security controls.

Cyber attack

A cyber attack is a deliberate attempt by an individual or group to breach, damage or disrupt:

- computer systems
- networks
- digital devices.

This is often for malicious purposes.

Addressing this finding

To address this finding, we have made:

- one recommendation to all agencies about strengthening the technical security controls on their known servers
- one recommendation to DGS about issuing guidance relating to minimum requirements for technical security controls for all Victorian government agencies.

2.
Our recommendations

We made 3 recommendations to address our findings. The relevant agencies have accepted the recommendations in full or in principle.

			Agency response(s)	
Finding: No agency has a complete and accurate server inventory				
All agencies	1	Improve their tracking of all IT servers by (where necessary): • using automated asset discovery tools • establishing and maintaining a centralised IT server asset register using appropriate server tracking software • assigning clear responsibility for the accuracy and completeness of IT server inventory.	Accepted in principle by Department of Health, Department of Families, Fairness and Housing, Department of Jobs, Skills, Industry and Regions and Department of Transport and Planning Accepted by all other agencies	
Finding: All agencies can improve the maturity of technical security controls applied to their known servers				
All agencies	2	Strengthen technical security controls by: • developing a plan to improve technical security controls applied to servers, informed by the findings identified in the management letter we sent to each agency • implementing improvements consistent with the plan.	Accepted in principle by Department of Energy, Environment and Climate Action, Department of Jobs, Skills, Industry and Regions and Department of Transport and Planning Accepted by all other agencies	
Department of Government Services	3	In consultation with relevant agencies, issue guidance to agencies that establishes requirements for: • effective tracking of server inventory • applying and maintaining technical security controls for servers • reviewing and testing the effectiveness of technical security controls • managing servers with operating systems that no longer receive mainstream support.	Accepted	

3.

Agencies' server inventories

No audited agency has a complete and accurate server inventory.

Automated asset discovery tools used by agencies do not capture all servers, and few agencies use reconciliations to crosscheck their server inventory. All agencies provided us with server inventory information that had either incomplete or duplicate entries.

If agencies are not accurately tracking all their servers, they do not have all the information they need to protect their IT infrastructure.

Covered in this section:

- Application of automated asset discovery tools
- Reconciliation of server inventory information
- Incomplete and inaccurate server information

Application of automated asset discovery tools

Maintaining visibility of IT assets

According to the *Victorian Government IT Asset Management Guidance*, agencies' IT asset registers should hold complete and correct data to avoid IT assets being overlooked. This guidance recommends using automated discovery or scanning tools to help agencies maintain visibility of IT infrastructure.

It can be difficult for one automated asset discovery tool to achieve complete and consistent coverage in a complex IT infrastructure environment such as in many Victorian Government agencies. Agencies may choose to use a range of automated discovery tools suitable to their server environment.

The MCSB

The MCSB is a globally accepted benchmark of best-practice security for a multi-cloud environment. It includes a set of recommendations for organisations to secure cloud services, including security controls and baselines.

The MCSB recommends that organisations track their asset inventory and their risks by using automated asset discovery tools to discover their assets. It recommends tagging and grouping assets based on their:

- service nature
- location
- other characteristics.

Agencies' use of automated asset discovery tools

We surveyed agencies to assess the technical security controls they apply to their servers. We asked agencies if they use automated asset discovery tools across their entire server environment.

In response to our survey ...	reported ...	across ...
3 agencies	that they do not use automated asset discovery tools	any of their servers.
2 agencies	using automated asset discovery tools	some of their servers.
4 agencies		their entire server environment.

This analysis relates to agency responses to our technical security controls survey (9 of 11 audited agencies provided a response).

We tested the settings of the automated asset discovery tools of the 4 agencies that reported using them across their entire server environment. We found that none had their automated asset discovery tools set up to scan for servers across their entire network.

This means that agencies may have servers they do not know about.

Reconciliation of server inventory information

Reconciliation processes

Three agencies carry out reconciliations to track their servers. These processes include:

- manually verifying server entries
- regular audits (including physical audits)
- using secondary tools to monitor server status and manually reflect updates in a master document.

An additional 2 agencies have reconciliation or audit processes for some, but not all, of their server environments.

Server reconciliations can help identify gaps in server inventories, but they are not considered best practice on their own. Best practice typically involves using automated asset discovery tools.

Incomplete and inaccurate server information

Agencies' server inventories

In January 2025, we asked all agencies to provide us with their server inventories for all on-premises and IaaS servers. We asked them to provide these in lists or in registers.

We asked agencies to include information relating to:

- server location (whether the server is a physical or virtual server)
- operating system and version
- host names.

The information we asked for is consistent with the MCSB, which recommends that assets are organised based on their:

- service nature
- location
- other characteristics.

We asked for information on servers managed by agencies and third-party providers. Cenitex provided information for servers it manages on behalf of audited agencies.

Incomplete and inaccurate server information

We analysed the server information agencies provided us and found that all agencies provided an incomplete server inventory. This means that the server inventory was missing information about its:

- operating system version name or number
- host name
- location.

Eight agencies also had duplicate records for the same server entry. The number of duplicate records across agencies ranged from 4 to over 1,000. Duplicates suggest the information has been entered or collated manually, which can increase the risk of inaccurate information.

Incomplete server inventory information can make it harder for agencies to identify and respond to risks that are not captured in this information. These risks include operating systems or servers not receiving mainstream support.

These findings highlight significant weaknesses in how agencies track their server environments.

Informed by our audit findings, some agencies did follow-up work to resolve missing and duplicated information.

Impact of incomplete and inaccurate information

For agencies to secure their servers and apply foundational technical security controls to them, they must first know what servers they have.

Without a complete and accurate server inventory, agencies cannot effectively manage their server security.

Agencies also cannot know what technical security controls are applied to servers that they do not know about.

4.

Servers' technical security controls

All agencies can improve the technical security controls applied to their known servers.

Based on our assessment against established industry benchmarks, the maturity level of technical security controls applied by all agencies to their known servers is low.

Most known servers are running operating systems that are not receiving mainstream support.

These factors increase the risk that agencies will not detect server vulnerabilities.

Given the weaknesses we identified in each agency's server inventory (as explained in Section 3), the following information reflects servers that the agencies know about.

Agencies' security controls and monitoring activities will only be fully effective if they are applied to all their servers.

Covered in this section:

- Maturity of technical security controls applied to servers
- Servers' operating systems
- Monitoring and reporting threats and vulnerabilities

Maturity of technical security controls applied to servers

Benchmarks and standards for technical security controls

Standard 11 of the *Victorian Protective Data Security Standards* requires Victorian Government departments to establish, implement and maintain ICT security controls.

The MCSB provides a globally accepted benchmark that reflects best-practice technical security controls for a multi-cloud environment.

We developed a model based on the MCSB. We used this to assess the maturity of agencies' technical security controls applied to their servers.

While the model is based on the MCSB, we also considered equivalent controls under other widely accepted industry benchmarks, such as those established by the:

- Center for Internet Security
- National Institute of Standards and Technology.

This provided a consistent framework to assess agencies' technical security controls.

VAGO's maturity model for server security

In our maturity model, we looked at all MCSB controls relevant to server security and grouped them into 5 key elements.

The ...	element is important because ...
operating system version	using a vendor-supported operating system ensures access to critical security updates and patches.
industry-standard hardened images	they provide a uniform approach for reducing server vulnerabilities.
industry security baselines	they establish a minimum security standard and help to assess if new or critical security controls are in place.
access control and patching	it limits unauthorised access and fixes known vulnerabilities.
backup and monitoring	it better enables an agency to identify, respond to and recover from security threats and risk.

Maturity levels range from level 1 at the lowest end through to level 5. These levels are based on the impact the controls have on the risk environment and are defined below.

- Level 1 (initial): high risk with lack of controls, or inconsistently applied basic compliance controls.
- Level 2 (managed): moderate risk with basic compliance controls.
- Level 3 (defined): moderate to low risk with some manual controls and slower response.
- Level 4 (proactive): low risk with strong, reliable controls.
- Level 5 (optimised): very low or minimal risk with highly secure controls.

Our maturity model is set out in full in Appendix D.

Industry-standard hardened images

A system image is a copy of a computer's entire system. Industry-standard hardened images are system images that have been preconfigured to meet industry best practices. This includes those in the Center for Internet Security's benchmarks and the National Institute of Standards and Technology's guidelines.

Patching

Patches are software and operating system updates that address security vulnerabilities within a program or product.

Agency assessments

We surveyed agencies to assess the technical security controls they apply within each of the 5 elements in our maturity model.

Nine agencies responded. We note that 2 agencies outsource their server management to Cenitex. These agencies did not provide a response to our survey. The technical security controls for these agencies are reflected in the survey responses provided by Cenitex.

Our assessment of the maturity of agencies' technical security controls is summarised in Figure 2.

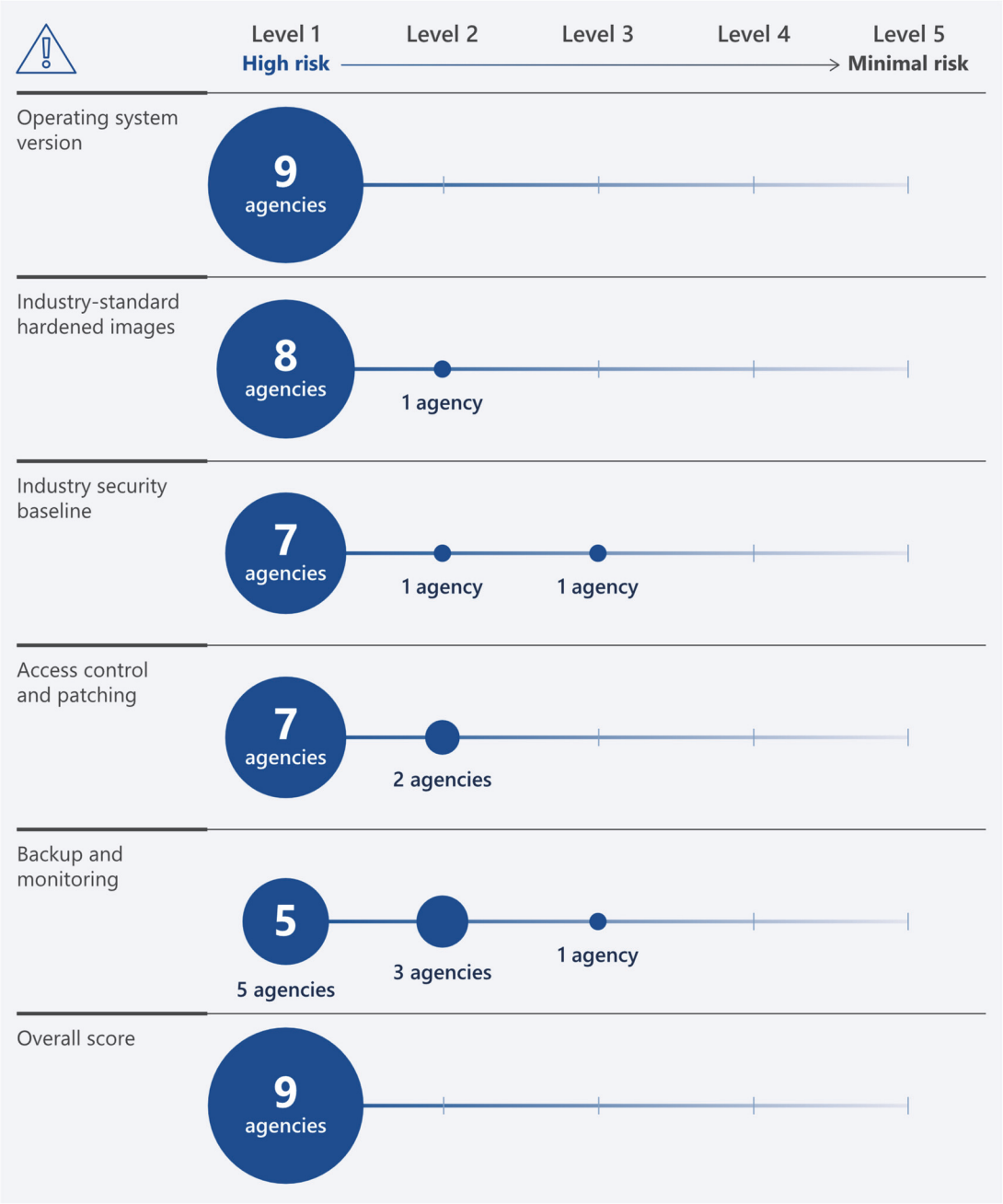
All agencies can improve the maturity of technical security controls applied to their known servers.

For overall maturity, we assessed all agencies as being at level 1, which is equivalent to a high-risk environment.

Across the 5 key elements of server security, we assessed all agencies as being at level 1 (the lowest level on our maturity model) for operating system version.

Some agencies achieved higher outcomes across other elements. For example, we assessed one agency at level 3 for industry security baselines.

Figure 2: Our assessment of agencies' technical security controls maturity



Note: Number represents number of agencies who reached that level for the particular element.
Source: VAGO.

Our assessment reflects a cumulative approach, which is consistent with the approach taken by the Australian Signals Directorate's Essential Eight model. This approach requires an organisation to implement all controls at a certain level to progress to the next.

For example, for an agency to reach level 3 maturity overall, it would need to have all level 3 and all lower-level technical security controls in place across the 5 elements. This recognises that gaps in these lower-level controls can undermine the effectiveness of more advanced protections elsewhere.

We made our assessments at an agency level. This means that we took the lowest level achieved by any business unit of an agency (where an agency provided this detail to us) as the agency's overall rating.

Impacts of low technical security controls maturity

Without sufficient and effective safeguards, agencies are exposed to increased risks of cyber attacks such as:

- unauthorised access
- information breaches
- operational disruptions.

During the audit, some agencies noted that they use 'compensating controls' not captured by the MCSB or equivalent standards. Some agencies may apply these controls where they cannot apply the recommended technical security control. These compensating controls include:

- internal policies
- security tools
- review processes.

We did not assess controls outside of our server security maturity model as this is not within the scope of this audit.

Improvements to agencies' technical security controls

Following the conduct phase of our audit, we asked agencies to update us on their planned initiatives to improve their technical security controls.

One agency plans to develop a cybersecurity controls and assurance framework, which will include controls around IT asset management as well as managing access to server accounts.

Another agency is establishing a cybersecurity committee. It will also implement a program to carry out:

- vulnerability management through server scanning and monitoring
- regular penetration testing to identify vulnerabilities in server security.

Another agency anticipates having automated asset discovery tools in place by November 2025.

Servers' operating systems

Importance of supported operating systems

The version of an operating system is a key indicator of a server's security maturity.

Servers can be running on operating systems that are either:

- in mainstream support (actively supported by the vendor)
- in extended support (receiving limited updates)
- unsupported (no longer receiving security updates, bug fixes or technical assistance).

Servers running operating systems that are in mainstream support typically:

- receive critical security updates
- receive the latest security features
- integrate with other protective tools.

Outdated or unsupported operating systems typically lack these capabilities.

Servers with operating systems that are unsupported or running on extended support may require increased monitoring and custom solutions or services. These could be costly and inefficient compared to supported operating systems. For example, servers on extended support require an end-of-life plan before the operating system becomes unsupported.

Operating system

An operating system is a program that runs on a computer and provides a software platform on which other programs can run.

Servers with unsupported operating systems

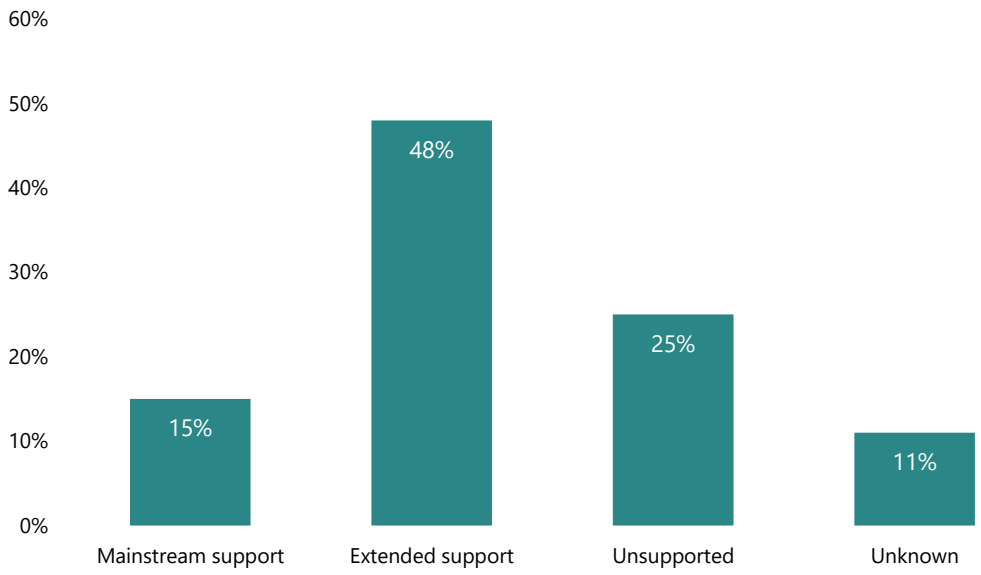
In January 2025, we asked agencies to provide us with their server inventory information, including the operating system and version for each server. We used this information to assess the status of support provided to operating systems running on known servers.

Our analysis of this information showed that 25 per cent of server entries reported by agencies had operating systems that are unsupported.

A further 11 per cent had unknown operating systems. Operating system names and numbers in these server records were either missing or incomplete. These servers are at higher risk of security breaches. This is shown in Figure 3.

All agencies reported some servers running unsupported operating systems or with an unknown status.

Figure 3: Status of operating systems across all agencies by percentage of servers



Note: Percentages do not add up to 100 per cent due to rounding.
Source: VAGO, based on agencies' server inventory information.

Servers with operating systems approaching end of life

We asked agencies 2 questions about how they manage servers using operating systems that are at, or approaching, end of life (unsupported).

We asked agencies if they have ...	and we found ...
a tool in place to track the lifecycle of server assets, including operating systems at end of life	4 agencies have this.
a process for managing operating systems that are approaching end of life	3 agencies (including 2 mentioned above) have this.

This analysis relates to agency responses to our technical security controls survey. Nine of 11 audited agencies provided a response.

Agencies that do not track the lifecycle of their assets, including if they are reaching end of life, will not know when their servers need to be updated or decommissioned.

Monitoring and reporting threats and vulnerabilities

Monitoring cyber threats

Victorian Government agencies are accountable for protecting their networks against cyber threats.

The implementation guidance for the *Victorian Protective Data Security Standards* recommends that agencies log system events and actively monitor them to detect potential security issues.

The guidance does not direct agencies to use a specific process or requirement for detecting threats. Instead, it is up to each agency to decide how they monitor and protect against cyber threats.

Cyber threat

Any circumstance or event affecting an information system that has the potential to negatively impact an organisation's operations, assets or individuals. This can be through:

- unauthorised access to information
- destruction of information
- disclosure of information
- modification of information
- denial of service.

All agencies monitor cyber threats and incidents

We assessed if all agencies monitor cyber threats and incidents. We found that all agencies have mechanisms in place to do so.

We found that all agencies:

- have an automated threat alert system in place
- have a cybersecurity incident register, or equivalent, to log incidents
- use intrusion and prevention detection systems. These are tools that agencies can use to protect their servers by blocking or detecting cyber threats.

Monitoring server vulnerabilities

Vulnerability scanning helps agencies identify security vulnerabilities, both known and potential.

The implementation guidance for the *Victorian Protective Data Security Standards* suggests that organisations carry out vulnerability management activities prioritised by risk. These activities can include:

- patch management
- penetration testing
- using continuous monitoring systems.

The *Victorian Government IT Asset Management Guidance* recommends that agencies receive regular information on vulnerabilities impacting their IT assets.

Not all agencies proactively manage server vulnerabilities

We asked agencies for information on how they monitor their servers for vulnerabilities. We found that not all agencies are proactively managing all their servers for vulnerabilities.

This may mean that agencies are not effectively reducing the risk of these servers being exploited by cyber attackers.

We found …	agencies …	which helps them to…
7*	monitor for vulnerabilities	identify where weaknesses and risks exist and reduce them accordingly.
8*	perform regular vulnerability scans to detect missing patches	keep their IT systems up to date with the latest security patches.
5*	prioritise patching based on a risk-scoring model	
7	conduct regular penetration testing of their servers	find and exploit vulnerabilities in IT systems. By simulating attacks, testers can identify weak spots in systems that could be exploited by real-world attackers.

*This analysis relates to responses to our technical security controls survey, to which only 9 out of 11 agencies responded.

Reporting on server threats and vulnerabilities

We assessed if all agencies report on their server threats and vulnerabilities.

We found that all agencies report internally on their monitoring of server threats and vulnerabilities at least monthly, with some agencies reporting this information fortnightly or weekly.

5.
Appendices

There are 4 appendices covering responses from audited agencies, information about how we perform our work, and our maturity model for server security.

Appendix A:
Submissions and comments

We have consulted with all agencies 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 relevant agency head.

Responses received

Response provided by the Chair, Cenitex

Level 9, 35 Collins Street ,
Melbourne, Victoria, 3000
(PO Box 2750)
ABN 56 375 109 796

Mr Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
31/35 Collins Street
Melbourne VIC 3000

Reference Number: 3490925

14/10/2025

Dear Mr Greaves

Re: Proposed report, the Cybersecurity of IT Servers

Thank you for your letter dated 1 October 2025 providing the *Proposed report, the Cybersecurity of IT Servers* for my consideration and comment.

I have considered the report, and I support the recommendations that align to Cenitex.

Cenitex has over the recent horizon taken significant investment to uplift and modernize the security, hosting and asset management of Cenitex and customer products.

Security is a key pillar of Cenitex services, and we continue to implement and refresh security services specifically tailored to the needs of government entities.

Cenitex's current strategy and deployment of servers to the cloud environment is significantly reducing the cyber security threat in the Cenitex environment.

Cenitex as the State Government's shared service provider, has a key role to play in the Cybersecurity of its own assets and as a provider of cybersecurity services to our customers. The continued challenge that is faced by Cenitex and its customers is to balance prudent investment with the ever-changing nature of cybersecurity along with the broad range of IT investment required.

I am pleased to provide the Cenitex action plan that outlines how Cenitex will implement the recommendations.

OFFICIAL: Sensitive

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

Should you or your team require any further information or assistance please contact Paul Kruspe Director Transformation on [redacted] or by email [redacted].

Yours sincerely,

[redacted]

Rodd Cunico

Chair

cc. Adrian Carbone, Acting Chief Executive Officer

cc. Paul Kruspe Director, Transformation and Strategic Programs

cenitex

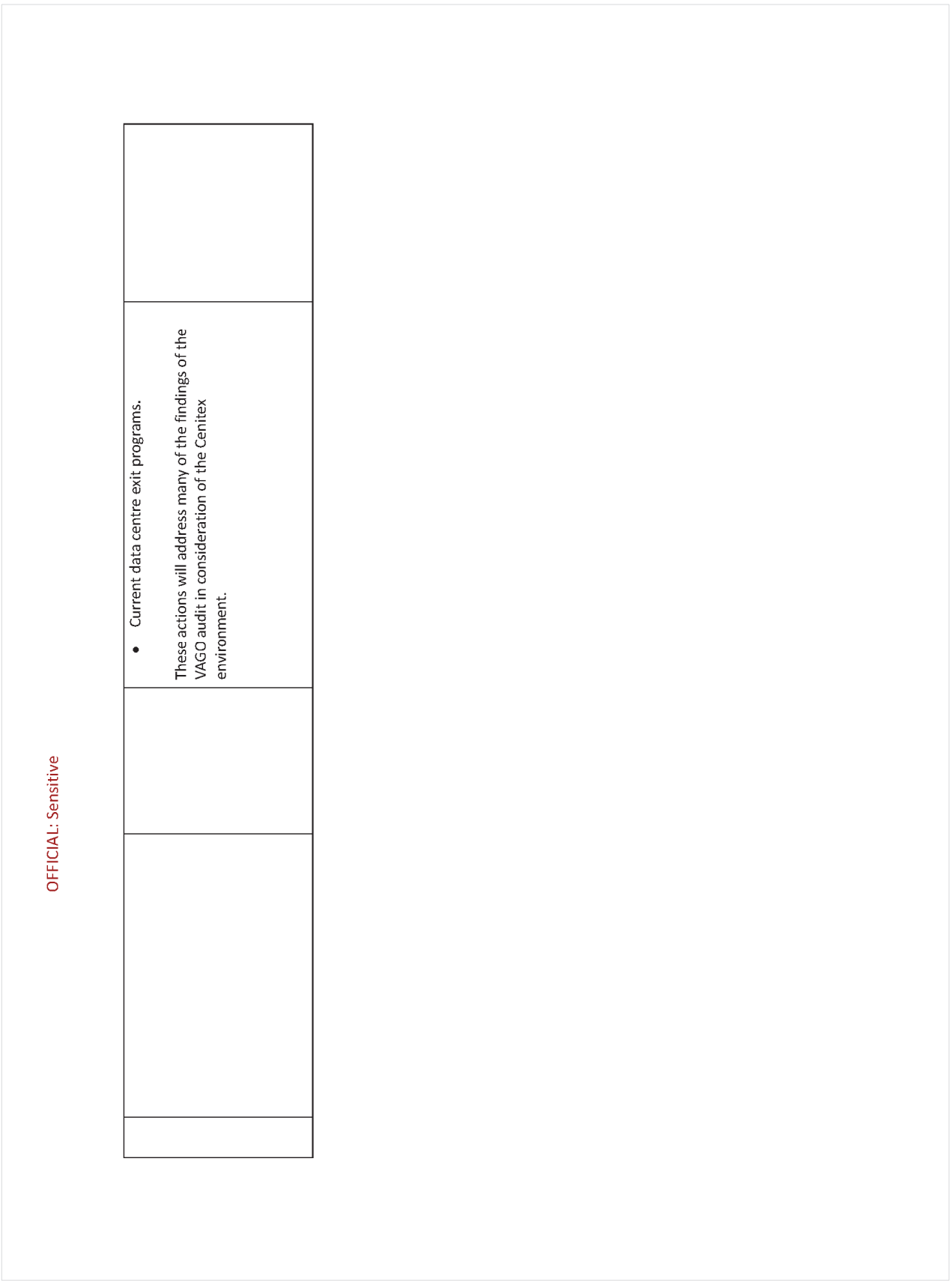
VICTORIA State Government

Cenitex action plan to address recommendations from *Cybersecurity of IT servers*

No.	VAGO recommendation	Acceptance	Agreed management actions	Target completion date

1	Improve their tracking of all IT servers by (where necessary):
	• using automated asset discovery tools
	• establishing and maintaining a centralised IT server asset register using appropriate server tracking software
	• assigning clear responsibility for the accuracy and completeness of IT server inventory.
		☒ Yes
		☐ No
		☐ In part
		☐ In principle
			Cenitex has in place all of the VAGO recommendations.
			
			This includes:
			• The use of multiple automated asset discovery tools
			• A central source asset register utilising contemporary server tracking software.
			• A robust governance process including:
			  ○ Asset register Health Metrics, which automatically run and report on a daily assessment of the completeness of the Server records.
			  ○ Focused process governance including a Data Quality Working Group & CMDB Working Group.
			In addition, the current program to exit the legacy Data centres will continue to increase the level of server compliance and increased cloud asset visibility.
				Completed

2	Strengthen technical security controls by: • developing a plan to improve technical security controls applied to servers, informed by the findings identified in the management letter we sent to each agency • implementing improvements consistent with the plan.	☒ Yes ☐ No ☐ In part ☐ In principle	Cenitex will reduce its on-premises servers as workloads are migrated under the strategic Multi-Cloud program and continue to prioritise its existing security compliance initiatives that will further strengthen security controls. Specifically, these will be addressed as part of in progress initiatives: • The Security Compliance program, • Scheduled operating system upgrades	December 2027


OFFICIAL: Sensitive
• Current data centre exit programs.
These actions will address many of the findings of the VAGO audit in consideration of the Cenitex environment.

Response provided by the Secretary, Department of Education

Department of Education

Secretary

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

COR25170857

Mr Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
[redacted]

Dear Mr Greaves

Proposed report on Cybersecurity of IT servers

Thank you for your letter of 1 October 2025 and the opportunity to comment on the proposed report for this audit. The department is committed to implementing and maintaining cybersecurity measures to protect its IT servers from threats.

The department has reviewed the proposed report, and an action plan to address the 2 recommendations applicable to the department is attached.

Should your staff wish to discuss the department's response, please contact Shamiso Mtenje, Executive Director, Integrity, Assurance and Executive Services Division on [redacted] or [redacted].

Yours sincerely

[redacted]

Tony Bates PSM
Secretary
15/10/2025

Encl.: DE's action plan

DE Final action plan: Cybersecurity of IT servers (with action owners)

#	Recommendations: That DE:	Response	#	The Department will:	By:
1	Improve their tracking of all IT servers, where necessary, by: • using automated asset discovery tools • establishing and maintaining a centralised IT server asset register using appropriate server tracking software • assigning clear responsibility for the accuracy and completeness of IT server inventory.	Accept	1.1	Enhance the use of discovery and server and cloud management tools to extend automated asset discovery across on-premise and cloud-based environments.	Sep 2027
			1.2	Establish and maintain a federated technology asset register governed under a technology asset management framework.	Dec 2026
			1.3	Implement a formal accountability framework for inventory and lifecycle management under a technology asset management framework.	Dec 2025
2	Strengthen technical security controls by: • developing a plan to improve technical security controls applied to servers, informed by the findings identified in the management letter for the department. • implementing improvements consistent with the plan.	Accept	2.1	Develop an action plan to improve technical security controls applied to servers, informed by the findings identified in the management letter.	Dec 2025
			2.2	Implement the actions as per the action plan and due dates to address the findings noted in the management letter.	Dec 2027

Response provided by the Secretary, Department of Energy, Environment and Climate Action

Department of Energy, Environment and Climate Action

PO Box 500, East Melbourne,
Victoria 8002 Australia

SEC-251000030

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

Via email: [redacted]

Dear Auditor-General

Proposed draft report – Cybersecurity of IT Servers

Thank you for your letter of 1 October 2025, inviting comment on your office's proposed draft report for the performance engagement: *Cybersecurity of IT Servers,* received 1 October 2025.

The Department of Energy, Environment and Climate Action (DEECA) recognises the need to effectively protect our IT servers from threats.

I can advise that DEECA accepts recommendation one outlined in the proposed draft report and accepts in-principle, recommendation 2 as this will be subject to DEECA's resource capacity. A proposed action plan for addressing these recommendations is enclosed.

I thank your staff for their work and look forward to a continued productive relationship with your office.

Yours sincerely

[redacted]

Kate Houghton PSM
Secretary

10 / 10 / 2025

Encl.

VICTORIA State Government

Official - Sensitive

Department of Energy, Environment and Climate Action – action plan to address recommendations from VAGO's report: *Cybersecurity of IT Servers*

No.	VAGO recommendation	Acceptance	Agreed management actions	Target completion date
1	Improve their tracking of all IT servers by (where necessary): • using automated asset discovery tools • establishing and maintaining a centralised IT server asset register using appropriate server tracking software • assigning clear responsibility for the accuracy and completeness of IT server inventory.	☒ **Yes** ☐ **No** ☐ **In part** ☐ **In principle**	1. DEECA will develop a policy that assigns clear responsibilities where all IT server owners are required to maintain accuracy and completeness of the centralised DEECA IT server register utilising existing IT server tracking software.	26 June 2026
2	Strengthen technical security controls by: • developing a plan to improve technical security controls applied to servers, informed by the findings identified in the management letter we sent to each agency • implementing improvements consistent with the plan.	☐ **Yes** ☐ **No** ☐ **In part** ☒ **In principle**	1. DEECA will develop a plan to improve its technical security controls applied to IT servers, as identified within the management letter. This will be based on the department's risk control priorities and resource capacity. 2. DEECA will develop a schedule for implementing the improvement plan for technical security controls applied to IT servers.	31 July 2026 30 October 2026

VICTORIA State Government | Energy, Environment and Climate Action

Response provided by the Secretary, Department of Families, Fairness and Housing

Secretary

Department of Families, Fairness and Housing

50 Lonsdale Street
Melbourne Victoria 3000
Telephone: 1300 475 170
GPO Box 1774
Melbourne Victoria 3001
www.dffh.vic.gov.au

VAGO File No: 34909 25

DFFH File No: BAC-CO-59183

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

Dear Mr Greaves

Thank you for providing the proposed report for VAGO's Cybersecurity of IT servers performance audit.

The Department of Families Fairness and Housing welcomes this report and supports the audit's findings, acknowledging the importance of cybersecurity and the protection of information held by the department.

The department has reviewed the proposed report and the two recommendations directed at all agencies. The department accepts in principle Recommendation 1 and accepts Recommendation 2, noting that implementation will involve working with the department's third-party vendors, and will be contingent on identifying funding.

I would like to take this opportunity to thank your staff for working collaboratively with the Department of Families, Fairness and Housing.

Yours sincerely

[redacted]

Peta McCammon
Secretary

16/10/2025

Encl.

DFFH action plan to address recommendations from *Cybersecurity of IT servers*

No.	VAGO recommendation	Acceptance	Agreed management actions	Target completion date
1	Improve their tracking of all IT servers by (where necessary): • **a)** using automated asset discovery tools • **b)** establishing and maintaining a centralised IT server asset register using appropriate server tracking software • **c)** assigning clear responsibility for the accuracy and completeness of IT server inventory.	☐ Yes ☐ No ☐ In part ☒ In principle	**a)** The department accepts the recommendation to use automated asset discovery tools. The department will work with our third-party vendors to enhance its tracking of IT servers. **b)** The department accepts in principle the establishment and maintenance of a centralised IT server asset register using appropriate server tracking software. Implementation is contingent on identifying funding. **c)** The department accepts the assignment of clear responsibility for maintaining an accurate and complete inventory of IT servers and will implement as a priority	**a)** 30 June 2026 **b)** 31 October 2026 **c)** 31 October 2025
2	Strengthen technical security controls by: • **a)** developing a plan to improve technical security controls applied to servers, informed by the findings identified in the management letter we sent to each agency • **b)** implementing improvements consistent with the plan.	☒ Yes ☐ No ☐ In part ☐ In principle	**a)** The department accepts this recommendation to develop a plan to improve technical security controls. Work is underway to identify server security risks, with a formal roadmap planned to prioritise mitigation from high to low risk. **b)** The department accepts this recommendation; Implementation of a plan will be contingent on identifying funding	**a)** 30 June 2026 **b)** 30 June 2027

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

Our ref: BSEC-250900155

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

By email: [redacted]

Dear Auditor-General

VAGO PROPOSED REPORT: CYBERSECURITY OF IT SERVERS PERFORMANCE AUDIT

Thank you for your letter dated 1 October 2025 enclosing the proposed report *Cybersecurity of IT Servers* for consideration and comment.

The Department of Government Services (DGS) acknowledges the report and accepts its findings. DGS is committed to continually improving its technical security controls and implementing the recommendations made by VAGO for DGS and its customer departments, including the Departments of Premier and Cabinet and Treasury and Finance.

I have enclosed a copy of DGS' action plan responding to the audit recommendations.

If your office requires further information, please have them contact Dovid Clarke, Chief Information Security Officer, DGS at [redacted].

Yours sincerely

[redacted]

Jo de Morton
Secretary

15 / 10 /2025

Enc DGS action plan to address recommendations in Cybersecurity of IT servers

DGS action plan to address recommendations in *Cybersecurity of IT servers*

No.	VAGO recommendation	Acceptance	Agreed management actions	Target completion date
1	Improve their tracking of all IT servers by (where necessary): • using automated asset discovery tools • establishing and maintaining a centralised IT server asset register using appropriate server tracking software • assigning clear responsibility for the accuracy and completeness of IT server inventory.	☒ Yes ☐ No ☐ In part ☐ In principle	Progressive deployment of automated asset discovery tools across the IT server environment to capture and reconcile all operating systems and applications that aligns with IT Asset Management Policy guidance. This work has already commenced.	31 December 2026
2	Strengthen technical security controls by: • developing a plan to improve technical security controls applied to servers, informed by the findings identified in the management letter we sent to each agency • implementing improvements consistent with the plan.	☒ Yes ☐ No ☐ In part ☐ In principle	1. Develop remediation plans for all servers running on legacy operating systems. Undertake a security review of legacy servers with the aim of protecting servers with layered security. 2. Implement improvement plans, informed by findings contained in the VAGO Management Letter, to address weaknesses in platform-specific technical security controls and departmental cyber security controls. 3. Collaborate with Cenitex and third-party vendors to implement technical security controls that meet whole-of-government minimum requirements (that will be determined in response to recommendation 3).	1. 31 December 2026 2. 30 June 2027 3. 31 December 2027
3	In consultation with relevant agencies, DGS should issue guidance to agencies that establishes requirements for: • effective tracking of server inventory • applying and maintaining technical security controls for servers • reviewing and testing the effectiveness of technical security controls • managing servers with operating systems that no longer receive mainstream support.	☒ Yes ☐ No ☐ In part ☐ In principle	DGS will develop whole-of-government guidance for the minimum requirements for technical security controls for all Victorian Government agencies.	30 June 2026

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: 34909 25

DH File No: BAC-CO-59186

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

Dear Mr Greaves

Thank you for providing the proposed report for VAGO's *Cybersecurity of IT servers* performance audit.

The Department of Health welcomes this report and supports the audit's findings, acknowledging the importance of cybersecurity and the protection of information held by the department and Victoria's health system.

The department has reviewed the proposed report and the two recommendations directed at all agencies. The department accepts in principle recommendation 1 and accepts recommendation 2, noting that implementation will involve working with the department's third-party vendors, and will be contingent on identifying funding.

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

Yours sincerely

[redacted]

Jenny Atta PSM
Secretary
15/10/2025

Attachment 1- DH Recommendation Action Plan - VAGO *Cybersecurity of IT servers*

DH action plan to address recommendations from *Cybersecurity of IT servers*

No.	VAGO recommendation	Acceptance	Agreed management actions	Target completion date
1	Improve their tracking of all IT servers by (where necessary): • **a)** using automated asset discovery tools • **b)** establishing and maintaining a centralised IT server asset register using appropriate server tracking software • **c)** assigning clear responsibility for the accuracy and completeness of IT server inventory.	☐ Yes ☐ No ☐ In part ☒ In principle	**DH** **a)** The department accepts the recommendation to use automated asset discovery tools. The department will work with its third-party vendors to enhance tracking of the department's IT servers. **b)** The department accepts in principle the recommendation for the establishment and maintenance of a centralised IT server asset register using appropriate server tracking software. Implementation is contingent on identifying funding. **c)** The department accepts the assignment of clear responsibility for maintaining an accurate and complete inventory of IT servers and will implement this action as a priority.	**DH** **a)** 30 June 2026 **b)** 31 October 2026 **c)** 31 October 2025
			HTS **a)** The department accepts in principle the recommendation to use automated asset discovery tools and has already partly implemented this. Full implementation is contingent on identifying funding. **b)** The department accepts in principle the establishment and maintenance of a centralised IT server asset register using appropriate server tracking software. Implementation is contingent on identifying funding. **c)** HTS currently has clear responsibilities in this area.	**HTS** **a)** 31 December 2028 **b)** 31 December 2028 **c)** Complete

No.	VAGO recommendation	Acceptance	Agreed management actions	Target completion date
2	Strengthen technical security controls by: • **a)** developing a plan to improve technical security controls applied to servers, informed by the findings identified in the management letter we sent to each agency • **b)** implementing improvements consistent with the plan.	☒ Yes ☐ No ☐ In part ☐ In principle	**DH** **a)** The department accepts this recommendation to develop a plan to improve technical security controls. Work is underway to identify server security risks, with a formal roadmap planned to prioritise mitigation from high to low risk. **b)** The department accepts this recommendation. Implementation will be contingent on identifying funding	**DH** **a)** 30 June 2026 **b)** 30 June 2027
			HTS **a)** The department accepts this recommendation and will develop a plan as a priority. **b)** The department accepts this recommendation. Implementation of a plan will be contingent on implementing recommendations 1a and 1b and identifying funding.	**HTS** **a)** 31 December 2025 **b)** 31 December 2028

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-2-25-27264

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

Dear Mr Greaves

CYBERSECURITY OF IT SERVERS PROPOSED REPORT

Thank you for your letter dated 1 October 2025 on the Cyber Security of IT Servers reasonable assurance performance audit.

The Department of Jobs, Skills, Industry and Regions (the department) acknowledges the proposed report and findings. Whilst the department does not agree with all the assessments made, the department remains committed to strengthening its cybersecurity posture and implementing the relevant recommendations.

Feedback on the management letter and the department's action plans to address the recommendations are provided as attachments to this correspondence.

If you require further information, your team can contact Karan Gill, Chief Audit Officer on [redacted] or [redacted].

Yours sincerely

[redacted]

Matt Carrick
Secretary

15/10/2025

VICTORIA State Government

DJSIR action plan to address recommendations from *Cybersecurity of IT servers*

No.	VAGO recommendation	Acceptance	Agreed management actions	Target completion date
1	Improve their tracking of all IT servers by (where necessary): • using automated asset discovery tools • establishing and maintaining a centralised IT server asset register using appropriate server tracking software • assigning clear responsibility for the accuracy and completeness of IT server inventory.	☐ Yes ☐ No ☐ In part ☒ In principle	DJSIR accepts this recommendation in principle and will undertake a detailed review of these controls as part of its Cyber Strategy. This will include assessment and identifying how each can be addressed either through current capability or funding for the uplift of these automated services. The assessment will be undertaken for DJSIR managed cloud platforms and not those hosted by Cenitex.	June 2026
2	Strengthen technical security controls by: • developing a plan to improve technical security controls applied to servers, informed by the findings identified in the management letter we sent to each agency • implementing improvements consistent with the plan.	☐ Yes ☐ No ☐ In part ☒ In principle	DJSIR accepts this recommendation in principle as it currently apply several industry controls including NIST, Essential 8 and VDPSS. The CIS Benchmark is another series of controls that can be applied where there may be gaps in the management of servers. DJSIR will undertake an assessment of the CIS Benchmark to identify opportunities to uplift our security framework for cloud systems including: • enforcing time-bound access for privileged actions • processes or policies relating to hardened images. Identified opportunities will be implemented in 2026-27 subject to implementation funding.	June 2026 for assessment June 2027 for implementation

Response provided by the Secretary, Department of Justice and Community Safety

Department of Justice and Community Safety

Secretary

Level 26
121 Exhibition Street
Melbourne Victoria 3000
Telephone: (03) 8684 0501
justice.vic.gov.au

Our ref: EBC 25092918

Mr Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Via email: [redacted]

Proposed report: Cybersecurity of IT servers

Dear Mr Greaves

Thank you for your letter of 1 October 2025 providing the proposed report and management letter for your audit on Cybersecurity of IT servers.

The department is committed to improving how it manages controls to mitigate the risk of cybersecurity incidents and threats.

Please see the attached action plan for addressing the 2 recommendations for all departments.

If you have any questions or require further information, please contact Julianne Brennan, Executive Director, Governance and Assurance on [redacted] or via email at [redacted].

Yours sincerely

[redacted]

Emma Cassar
Secretary

20/10/2025

DJCS action plan

Cybersecurity of IT servers

#	VAGO recommends that all agencies:	Response	#	DJCS will:	By:
1	Improve their tracking of all IT servers (where necessary): • using automated asset discovery tools • establishing and maintaining a centralised IT server asset register using appropriate server tracking software • assigning clear responsibility for the accuracy and completeness of IT server inventory.	Accept	1	Improve tracking of all DJCS IT servers by: • using automated asset discovery tools • establishing and maintaining a centralised IT server asset register using appropriate server tracking software • assigning clear responsibility for the accuracy and completeness of IT server inventory.	30-Jun-27
2	Strengthen technical security controls by: • developing a plan to improve technical security controls applied to servers, informed by the findings identified in the management letter we sent to each agency • implementing improvements consistent with the plan.	Accept	2	• Use a risk-based approach to develop a plan to address the key/high-risk security control weaknesses. • Execute the plan to remediate those weaknesses.	30-Jun-27

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

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

BSEC-250900432

By email: [redacted]

Dear Auditor-General

Thank you for your letter dated 1 October 2025 enclosing the proposed report *Cybersecurity of IT Servers* for consideration and comment.

The Department of Premier and Cabinet (DPC) acknowledges the report and accepts its findings. DPC is committed to continually improving our technical security controls and implementing the recommendations from VAGO. We are working with the Department of Government Services (DGS), our shared services provider, to address the recommendations.

I have enclosed a copy of DGS' action plan prepared by DGS in response to the recommendations of the audit.

Should your office require further information, they may contact Dovid Clarke, Chief Information Security Officer, DGS at [redacted]

Yours sincerely

[redacted]

Jeremi Moule
Secretary

15 / 10 / 2025

Encl.

VICTORIA State Government

DGS action plan to address recommendations from *Cybersecurity of IT servers* for DPC, DTF and DGS

No.	VAGO recommendation	Acceptance	Agreed management actions	Target completion date
1	Improve their tracking of all IT servers by (where necessary): • using automated asset discovery tools • establishing and maintaining a centralised IT server asset register using appropriate server tracking software • assigning clear responsibility for the accuracy and completeness of IT server inventory.	☒ Yes ☐ No ☐ In part ☐ In principle	1. Deploy asset discovery tools across the IT server environment to capture and reconcile all operating systems and applications that align with internal IT Asset Management Policy guidance.	1. 31 December 2026
2	Strengthen technical security controls by: • developing a plan to improve technical security controls applied to servers, informed by the findings identified in the management letter we sent to each agency • implementing improvements consistent with the plan.	☒ Yes ☐ No ☐ In part ☐ In principle	1. Develop remediation plans for all servers running on legacy operating systems; and undertake a security review of legacy servers with the aim of protecting servers with layered security. 2. Implement improvement plans, informed by findings contained in the VAGO Management Letter, to address weaknesses in platform-specific technical security controls and departmental cyber security controls. 3. Collaborate with Cenitex and third-party vendors to implement technical security controls that meet WOVG minimum requirements.	1. 31 December 2026 2. 30 June 2027 3. 31 December 2027

Response provided by the Secretary, Department of Transport and Planning

Department of Transport and Planning

GPO Box 2392
Melbourne, Victoria 3001 Australia

Ref: BSEC-1-25-4326

Mr Andrew Greaves
Auditor-General of Victoria
Victorian Auditor-General's Office
Level 31, 35 Collins Street
MELBOURNE VIC 3000
E: [redacted]

Dear Mr Greaves

Victorian Auditor-General's Office - Cybersecurity of IT servers - Proposed report

Thank you for your letter of 1 October 2025 inviting the Department of Transport and Planning (the Department) to respond to the *Cybersecurity of IT servers* proposed report (the Report).

The Department manages cyber risks in accordance with Victorian Government standards, policy and processes. On behalf of the Department, I acknowledge the Report's findings that there are opportunities to strengthen how agencies track their server environments and to improve the maturity of technical security controls for servers examined in this audit.

The Department has made significant investment in its Trusted and Secure program which is designed to mature the Department's cyber environment. Initiatives continue to be added or evolved as the cyber landscape continuously changes and gaps in our maturity are identified.

The Department accepts both of the Report's recommendations in principle and has prepared an action plan which is enclosed with this letter.

Thank you for the opportunity to comment on the Report.

[redacted]
Jeroen Weimar
Secretary

Date: 15 October 2025

Enc: DTP action plan - Cybersecurity of IT servers

DTP action plan

Cybersecurity of IT servers

The Department of Transport and Planning (DTP) action plan to address the recommendations from *Cybersecurity of IT servers*:

No	VAGO recommendation	DTP response	Due date
1	All agencies to improve their tracking of all IT servers by (where necessary): – Using automated asset discovery tools – Establishing and maintaining a centralised IT server asset register using appropriate server tracking software – Assigning clear responsibility for the accuracy and completeness of IT server inventory.	**Accepted in principle** The Department of Transport and Planning (DTP) will improve tracking of all IT servers hosted in an enterprise datacentre or IaaS environment by: – Using native asset discovery tools for cloud platforms. – Establishing and maintaining a centralised IT server asset register consolidating all hosting environments. – Assigning clear responsibility for the accuracy and completeness of IT server inventory.	31 March 2027
2	All agencies to strengthen technical security controls by: – Developing a plan to improve technical security controls applied to servers, informed by the findings identified in the management letter we sent to each agency – Implementing improvements consistent with the plan.	**Accepted in principle** DTP will strengthen technical security controls for servers hosted in an enterprise datacentre or IaaS environment by: – Developing a plan to improve technical security controls applied to servers, informed by the findings identified in the management letter. – Implementing improvements consistent with the plan.	31 March 2027

Response provided by the Secretary, Department of Treasury and Finance

Department of Treasury and Finance

1 Treasury Place
Melbourne Victoria 3002 Australia
Telephone: +61 3 9651 5111
dtf.vic.gov.au

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

BORG-250900534

By email: [redacted]

Dear Auditor-General

VAGO PROPOSED REPORT: CYBERSECURITY OF IT SERVERS PERFORMANCE AUDIT

Thank you for your letter dated 1 October 2025 enclosing the proposed report *Cybersecurity of IT Servers* for consideration and comment.

The Department of Treasury and Finance (DTF) acknowledges the report and accepts its findings. DTF is committed to continually improving its technical security controls and implementing the recommendations from VAGO. We are working with the Department of Government Services (DGS), our shared services provider, to address the recommendations.

I have enclosed a copy of DTF's action plan prepared by DGS in response to the recommendations of the audit.

Should your office require further information, they may contact Dovid Clarke, Chief Information Security Officer at [redacted]

Yours sincerely

[redacted]

Chris Barrett
Secretary

15/10/2025

Encl.

OFFICIAL

DGS action plan to address recommendations from *Cybersecurity of IT servers* for DTF

No.	VAGO recommendation	Acceptance	Agreed management actions	Target completion date
1	Improve their tracking of all IT servers by (where necessary): • using automated asset discovery tools • establishing and maintaining a centralised IT server asset register using appropriate server tracking software • assigning clear responsibility for the accuracy and completeness of IT server inventory.	☒ Yes ☐ No ☐ In part ☐ In principle	Progressively deploy automated asset discovery tools across the IT server environment to capture and reconcile all operating systems and applications that aligns with internal IT Asset Management Policy guidance.	31-December-2026
2	Strengthen technical security controls by: • developing a plan to improve technical security controls applied to servers, informed by the findings identified in the management letter we sent to each agency • implementing improvements consistent with the plan.	☒ Yes ☐ No ☐ In part ☐ In principle	1. Develop remediation plans for all servers running on legacy operating systems. Undertake a security review of legacy servers with the aim of protecting servers with layered security. 2. Implement improvement plans, informed by findings contained in the VAGO management letter, to address weaknesses in platform-specific technical security controls and departmental cyber security controls 3. Collaborate with Cenitex and third-party vendors to implement technical security controls that meet WOVG minimum requirements	1. 30-June-2026 2. 30-June-2027 3. 31-December-2027

Appendix B:
Abbreviations, acronyms and glossary

Abbreviations

We use the following abbreviations in this report:

Abbreviation	Full spelling
server	IT server

Acronyms

We use the following acronyms in this report:

Acronym	Full spelling
DGS	Department of Government Services
DH	Department of Health
IaaS	infrastructure as a service
ICT	information and communications technology
MCSB	Microsoft cloud security benchmark
VAGO	Victorian Auditor-General's Office

Glossary

The following terms are included in or relevant to this report

Term	Explanation
Level of assurance	This is a measure of the confidence we have in our conclusions. The quality and quantity of evidence we obtain affects our level of assurance. We design our work programs with the information needs of our report users in mind. We consider if we need to provide them with reasonable assurance or if a lower level of assurance may be appropriate.
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, 'nothing has come to our attention to indicate there is a problem.' See our assurance services fact sheet for more information.
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 draw a conclusion against an objective with a high level of assurance. We call these **performance audits**. See our assurance services fact sheet for more information.

Appendix C:
Audit scope and method

Scope of this audit

Who we examined

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

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

Our audit objective

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

What we examined

We examined if agencies:

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

We did not examine:

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

Aspects of performance examined

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

In this audit we focused on the following aspects:

Economy	Effectiveness	Efficiency	Compliance
○	●	○	○

Key:

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

Conducting this audit

Assessing performance

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

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

Our methods

As part of the audit, we:

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

Level of assurance

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

Compliance

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

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

Cost and time

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

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

Appendix D:
VAGO's maturity model for server security

Figure D1: VAGO's maturity model for server security

Maturity level	Operating system version	Industry-standard hardened images	Industry security baseline	Access control and patching	Backup and monitoring	Risk level
Level 1: initial (basic)	Unsupported operating system (e.g. 2008, 2012)	No	None	No patching or role-based access control	No automated backups or monitoring	High
Level 2: managed (basic compliance)	Extended supported operating system (e.g. 2016, 2019)	• Some images hardened • No automated configuration management	Minimal (only using default security policies)	• Manual patching • Minimal access control	Basic backups and logging	Moderate
Level 3: defined (standardised)	Mostly oldest supported operating system (e.g. 2022)	• All critical servers use hardened images • Automated configuration management implemented	Security baseline applied, such as: • Microsoft Security Baseline • Center for Internet Security technical implementation guide	• Regular patching • Role-based access control and least-privilege access	• Automated backups • Logging implemented	Moderate –low
Level 4: proactive (hardened)	Mostly latest supported operating system (e.g. 2025)	Most servers (more than 65%), including all critical servers, use hardened images, with automated configuration management	Customised security baseline based on industry standard	• Automated patching • Privileged access management solution	• Full backup/ restore • SIEM monitoring	Low
Level 5: optimised (highly secure)	Only latest supported operating system (e.g. 2025)	Hardened images across all, with automated configuration management	Continuous monitoring with customised baselines	• Continuous patching • Privileged access management • Privileged access workstations	• Full data protection • 24/7 security operations centre	Very low

Source: VAGO, based on the MCSB.

Auditor-General's reports tabled in 2025–26

Report title	Tabled
Delivering Savings Under the COVID Debt Repayment Plan (2025–26: 1)	July 2025
Planned Surgery in Victoria (2025–26: 2)	August 2025
Financial Management of Local Councils (2025–26: 3)	August 2025
Responses to Performance Engagement Recommendations: Annual Status Update 2025 (2025–26: 4)	September 2025
Relief and Recovery Funding for the 2022 Floods (2025–26: 5)	October 2025
Cybersecurity of IT Servers (2025–26: 6)	October 2025

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