Office of the Auditor General
Serving the Public Interest

Report 9: 2023-24 | 6 December 2023

INFORMATION SYSTEMS APPLICATION AUDIT

Implementation of the Essential Eight Cyber Security Controls

Office of the Auditor General
Western Australia

Audit team:
Aloha Morrissey
Kamran Aslam
Paul Tilbrook
Michael Chumak
Ben Goodwin
Aidan Orr
Information Systems Audit team

National Relay Service TTY: 133 677
(to assist people with hearing and voice impairment)

We can deliver this report in an alternative format for
those with visual impairment.

ISSN: 2200-1913 (print)
ISSN: 2200-1921 (online)

The Office of the Auditor General acknowledges the traditional custodians throughout Western Australia and their continuing connection to the land, waters and community. We pay our respects to all members of the Aboriginal communities and their cultures, and to Elders both past and present.

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Implementation of the Essential Eight Cyber Security Controls

Report 9: 2023-24
6 December 2023

This page is intentionally left blank

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

IMPLEMENTATION OF THE ESSENTIAL EIGHT CYBER SECURITY CONTROLS

This report has been prepared for submission to Parliament under the provisions of sections 24 and 25 of the *Auditor General Act 2006*.

Information systems audits focus on the computer environments of entities to determine if these effectively support the confidentiality, integrity and availability of information they hold.

This audit assessed the progress made by 10 State government entities to implement the Australian Signals Directorate's Essential Eight controls as required by the *WA Government Cyber Security Policy*. We assessed entities' control maturity and compared this with the self-assessments they provided to the Office of Digital Government in December 2022.

I wish to acknowledge the entities' staff for their cooperation with this audit.

CAROLINE SPENCER
AUDITOR GENERAL
6 December 2023

Contents

Auditor General's overview

Recent cyber attacks have highlighted the need for cyber security to be a key strategic priority across the public and private sectors. As State government entities deliver important services to the public through internet-facing systems, they can be subject to attacks. Further, a secure digital environment is vital to Australia's national interest, social confidence and cohesion and economic prosperity.

In response to concerns raised by this Office over some years, the State Government formed the Office of the Government Chief Information Officer in 2015, now the Office of Digital Government (DGov), to lead and support digital transformation of State entities and build their cyber security capabilities. DGov has played a crucial role in raising the sector's awareness of contemporary IT and cyber security practices. One of its key initiatives requires entities to implement the Australian Signals Directorate's Essential Eight controls and report their maturity levels through annual self-assessments.

This audit examined the progress made by 10 State entities to implement Essential Eight controls and the accuracy of their self-assessments reported to DGov. It provides useful insights on the quality of information reported to DGov, who is already analysing and actioning the report findings.

While all the audited entities have started their Essential Eight journey, considerable work is needed to fully implement these essential controls. In most instances, we found controls were only partially implemented or not working as expected, leaving entities vulnerable.

We also found most entities were overly optimistic in completing their Essential Eight maturity self-assessments. This presented an inaccurate and overconfident picture of their own readiness, and also the sector's maturity in cyber security. Entities need to have an accurate understanding of their maturity to prioritise and address weaknesses, and correctly inform the government's perception of the State's cyber risk exposure. It is not uncommon, however, for entities to be overconfident when self-assessing, a trend noted by other jurisdictions in Australia.[1]

Indeed, given that, I decided to subject my own Office's DGov reporting to the same audit scrutiny. While my Office's self-assessments were more accurate than the sector average, we did identify some room for improvement, which we have addressed.

I am pleased that the government is increasingly focused on cyber security and is continuing to build the skill base and digital resilience across the public sector. I also acknowledge the Australian Cyber Security Centre, which provides cyber security guidance, tools and assessment materials to implement and assess Essential Eight controls.

I encourage chief executives, chief information officers, audit committees and boards to maintain focus on building cyber resilience, and use insights from this report to probe and monitor their maturity in this area.

[1] Parliament of Australia, *Report 497 Inquiry into Commonwealth Financial Statements 2021-22*, APH website, 2023, accessed 22 November 2023, p. 30. and Audit Office of New South Wales, *Cyber Security NSW: governance, roles, and responsibilities*, NSW Audit Office website, 2023, accessed 2 October 2023, p. 25.

Executive summary

Introduction

This audit assessed the progress made by 10 State government entities to implement the Australian Signals Directorate's (ASD) Essential Eight[2] controls as required by the *WA Government Cyber Security Policy*.[3] We assessed entities' control maturity and compared this with the self-assessments they provided to the Office of Digital Government (DGov) in December 2022.

The 10 audited entities provide a range of essential services to the Western Australian public and hold large amounts of sensitive and personal data. We have not named the audited entities so as not to expose those with weaknesses to malicious threat actors. During the audit we informed DGov of our emerging findings so it could incorporate learnings into its approach to entities' 2023 self-assessments.

Background

State government entities provide unique and essential services to the public that increasingly rely on a range of information and operational technology systems for their delivery. Securing these systems is important to protect the social and economic wellbeing of the people of this state and Australia's national security interests.

Malicious cyber activity is a growing issue around the world. In 2022-23, approximately 94,000 cybercrime reports were made to law enforcement and the ASD's Australian Cyber Security Centre (ACSC[4]) responded to over 1,100 incidents, 43% of which were from Australian public sector entities.[5] We also regularly report cyber security and system control weaknesses in our annual information systems reports, particularly in the management of vulnerabilities and access, endpoint protection, network security, and a lack of adequate backup processes.

To help protect entities from malicious cyber activity, the ASD has developed a set of 37 mitigation strategies[6] (controls), prioritised by their security effectiveness (Figure 1). The eight most effective controls are known as the Essential Eight. As the Essential Eight will not mitigate against all cyber threats, the ASD also recommends additional controls.

Source: OAG based on ACSC information

Figure 1: Cyber threat mitigation controls

[2] Australian Government, *Essential Eight*, ASD website, 2023, accessed 20 September 2023.

[3] Department of the Premier and Cabinet, *WA Government Cyber Security Policy*, DPC website, 2021, accessed 3 October 2023.

[4] The ACSC is an Australian Government department, part of ASD, provides cyber security advice and support on cyber security.

[5] Australian Government, *ASD Cyber Threat Report 2022-2023*, ASD website, 14 November 2023, accessed 15 November 2023.

[6] Australian Government, *Strategies to Mitigate Cyber Security Incidents*, ASD website, 1 February 2017, accessed 20 September 2023.

Figure 2 shows the Essential Eight controls which provide entities with a security baseline to mitigate and protect against the majority of cyber security threats.

Source: OAG based on ACSC information

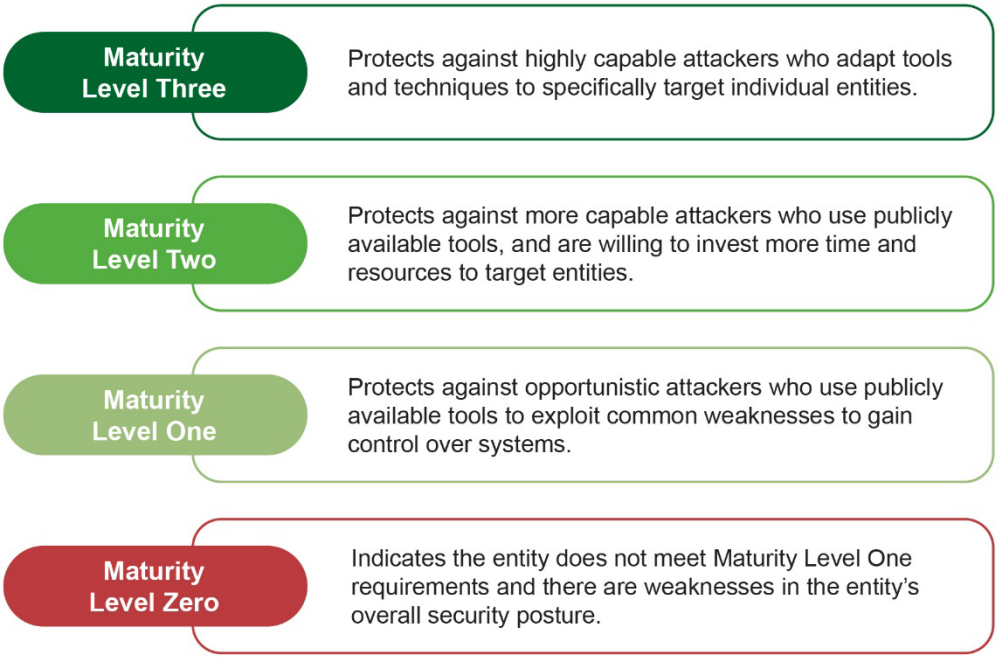
Figure 2: ACSC Essential Eight controls

The ACSC has defined four Essential Eight maturity levels that represent progressive control implementation and increasing effectiveness (Figure 3). Each maturity level has unique requirements that build on those of the previous level. We assessed entities against the maturity model used by entities to report self-assessments to the DGov in December 2022 (Appendix 1).

The ACSC has recently updated[7] its Essential Eight maturity model to protect entities from modern threats. It also provides free tools and guidance to help entities implement and assess their control maturity.[8]

[7] Australian Government, *Essential Eight Maturity Model Changes*, ASD website, 27 November 2023, accessed 28 November 2023.

[8] Australian Government , *Australian Signals Directorate's Cyber Security Partnership Program*, ASD website, n.d., accessed 2 October 2023.



Source: OAG based on ACSC information

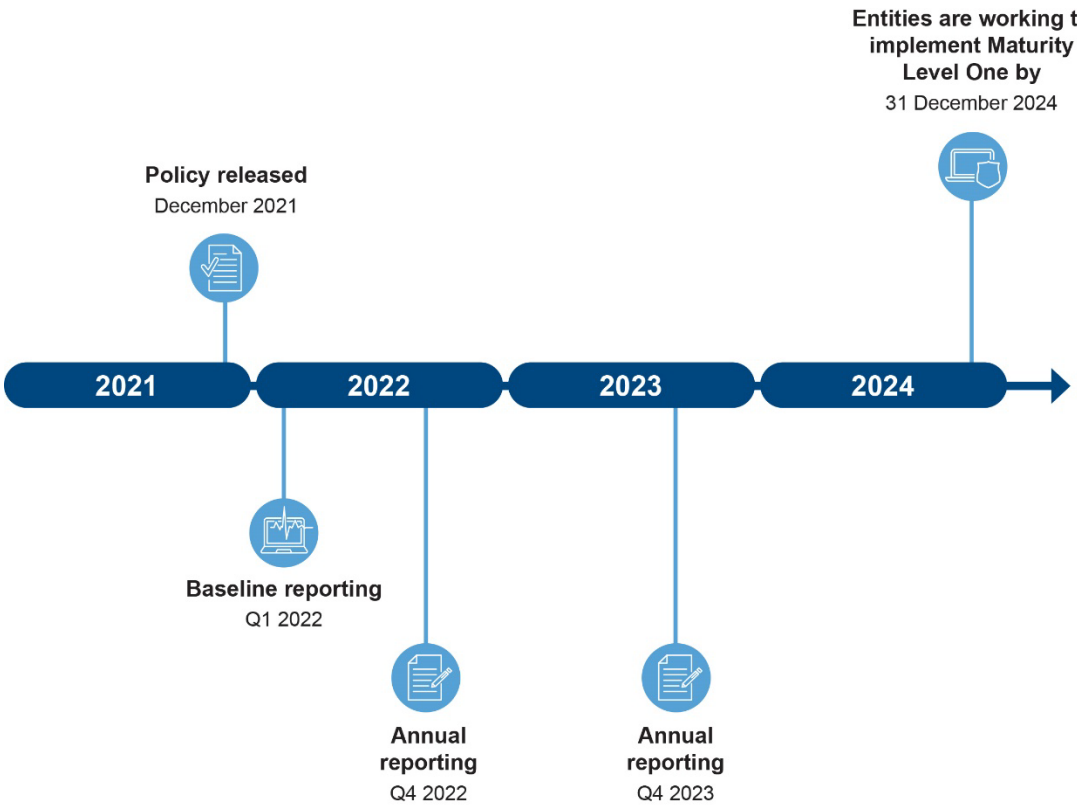
Figure 3: Essential Eight maturity levels

DGov has an important central role to lead, support and coordinate the digital transformation of State entities and build their cyber security capabilities. It also administers the WA Government's Digital Capability Fund aimed at driving strategic and targeted investment in digital transformation and assist entities to upgrade their legacy systems.

In December 2021, DGov released the *WA Government Cyber Security Policy* to improve the security posture of State entities. The policy requires State entities to implement the Essential Eight controls at least to a Maturity Level One. Entities are working towards implementing these controls by December 2024.

DGov requires entities to complete an annual implementation report which includes a self-assessment spreadsheet on their progress and maturity in implementing the Essential Eight controls. These self-assessments are then compiled by DGov into a whole-of-government cyber security progress report for their Minister. DGov does not verify the entity self-assessments when compiling the report.

Entities provided a baseline self-assessment report to DGov in March 2022 and their first annual implementation report in the fourth quarter of 2022 (Figure 4). The next round of annual reporting is due to DGov on 15 December 2023, which includes requirements from an updated version of the ACSC Essential Eight maturity model.



Source: OAG based on DGov information

Figure 4: Essential Eight implementation and reporting timeline

Conclusion

Mandatory implementation of the Essential Eight controls is an important WA State Government cyber security policy initiative to improve the sector's cyber capability and resilience. Through monitoring how entities are progressing with implementation, DGov continues to raise entities' awareness of the importance of controls to mitigate and protect against cyber security threats.

While the 10 entities we audited had started to implement the Essential Eight controls, more work is needed if entities are to achieve the *WA Government Cyber Security Policy* objectives. Five entities had not achieved Maturity Level One or higher in any control, and no entity had achieved Maturity Level One or higher in all controls. Weaknesses in an entity's cyber security leave it exposed to the threat of data breaches, unauthorised access and disruption to their systems and services. However, upgrading or replacing large legacy systems takes time and often requires significant planning and resources.

Most entities did not have an accurate understanding of their maturity against the Essential Eight controls. Our comparison of entities' Essential Eight maturity self-assessment to our assessments found seven entities overstated their maturity in one or more controls. This meant information reported by DGov to Government presented an inaccurate and potentially overconfident picture of the sector's cyber security readiness. Entities need to have an accurate understanding of their cyber security to appropriately prioritise and address weaknesses and mitigate risks.

DGov is aware of issues impacting the accuracy of entity self-assessments. It has already commenced a review of its guidance and tools to assist entities to more accurately assess their maturity. We note that existing ACSC guidance, tools and assessment materials can be directly accessed by entities to help them understand their security posture and accurately report to DGov.

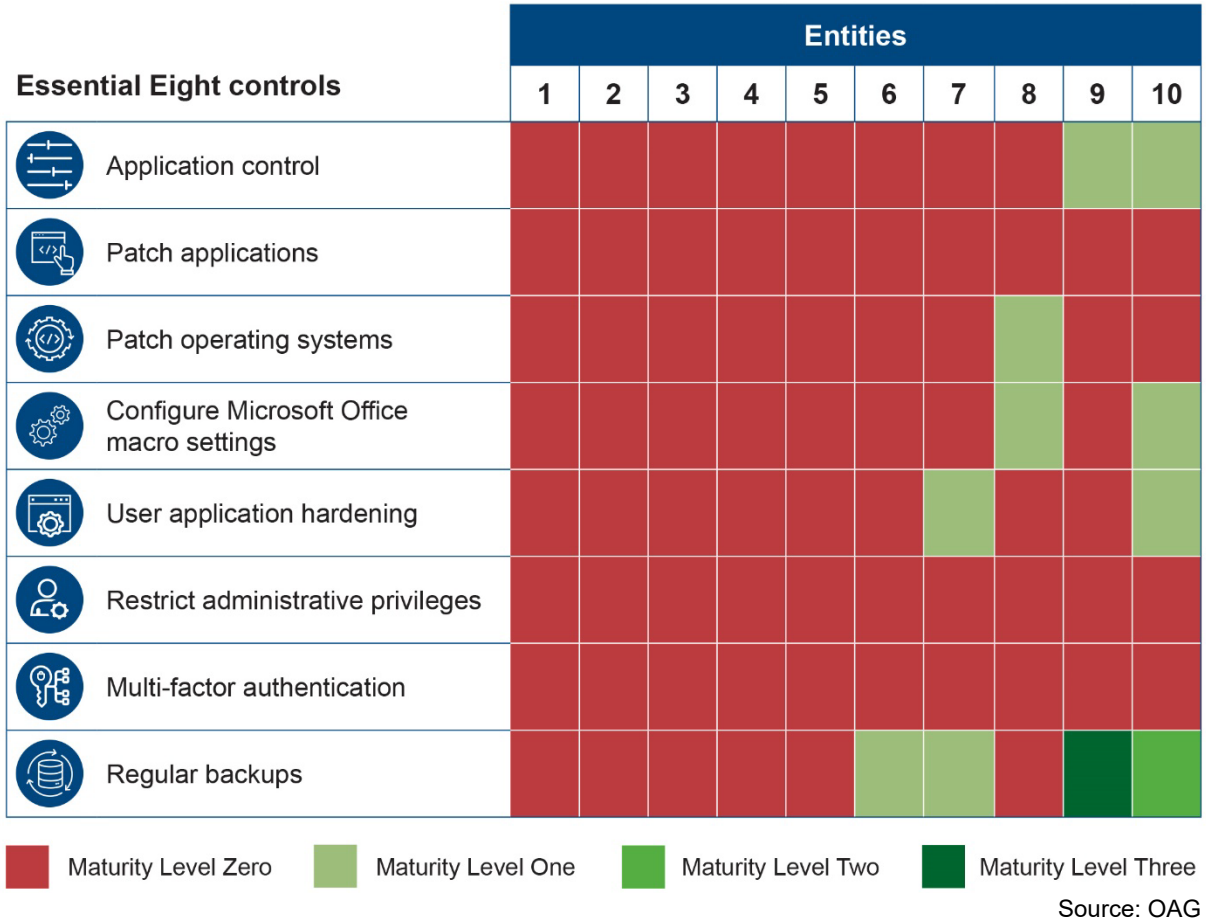
Findings

Entities have started to implement controls but more work is needed

None of the 10 audited entities had reached Maturity Level One or higher in all controls. Work is needed to achieve Maturity Level One and effectively protect entities from opportunistic threats.

Concerningly, we also found that five entities had not achieved Maturity Level One or higher in any controls, and none of the entities achieved Maturity Level One in patch applications, restrict administrative privileges and multi-factor authentication (Figure 5). Entities have either not implemented controls, or the controls they have implemented are not effectively designed or configured.

Figure 5 summarises the findings of our Essential Eight assessments at the 10 entities. We also provide a comparison of entities' self-assessments to our assessments in each control in Figure 6.



Source: OAG

Figure 5: Our assessment of Essential Eight controls maturity at 10 entities

Examples are provided below to show why entities failed to meet Maturity Level One in each of the Essential Eight controls.

Application control

Application control prevents the execution of malicious programs and scripts that attackers use to breach computer networks.

Two of the 10 entities had achieved Maturity Level One, the remaining eight entities were at Maturity Level Zero. At these eight entities we were able to run various unapproved executables[9] and scripts[10] from standard user profiles and temporary folders.

Patch applications

Patch applications is the continual process of identifying application vulnerabilities and applying software updates to prevent an attacker from compromising key systems and networks using known security vulnerabilities.

None of the 10 entities had achieved Maturity Level One. Our testing showed most entities were using unsupported applications and had vulnerabilities dating back several years. Four entities also had unsupported internet-facing applications, which further increase their exposure.

While all entities were using a vulnerability scanner, not all were scanning frequently enough (daily for internet-facing services and fortnightly for office productivity suites etc.).

Threat actors can quickly exploit newly identified vulnerabilities to gain control of networks and systems. It is imperative that entities identify and mitigate these vulnerabilities quickly.

Patch operating systems

Patch operating systems is the process of keeping workstations, servers and network devices up-to-date with software to maintain security and prevent attackers from using known security vulnerabilities to compromise systems.

One entity had achieved Maturity Level One in this control. We found common weaknesses at the remaining entities, including:

- vulnerability scans were not run frequently enough (daily for internet-facing services and fortnightly for other workstations, servers and network devices in line with Maturity Level One requirements)
- use of unsupported and legacy operating systems which are generally costly to maintain and can lead to operational disruptions.

[9] Executable is any file or program that can run on a computer.

[10] Script is a set of instructions to achieve a task by controlling various computer programs.

Configure Microsoft Office macro settings

Macros are pieces of code used by applications to automate tasks.

Attackers can use macros to introduce malicious code and gain unauthorised network and system access.

Two of the 10 entities had achieved Maturity Level One in this control. We found common weaknesses at the remaining entities, including:

- enabled macros without a demonstrated business requirement or entities had not identified users with a business need to use macros
- macros originating from the internet were not effectively blocked
- users could bypass macro controls configured by the entity as they were not prevented from changing security settings.

User application hardening

User application hardening reduces the 'attack surface' threat actors can use to deploy malicious software onto systems (e.g. workstations).

Application hardening limits the opportunities for attacks to occur by removing unnecessary system applications and placing restrictions on application functions that are vulnerable to malicious use.

Two entities achieved Maturity Level One in this control. We found common weaknesses at the remaining entities, including:

- web browsers were not prevented from processing java or advertisements from the internet
- continued use of obsolete Internet Explorer[11] (IE11) to load websites and content from the internet.

In addition, while some entities effectively secured the Microsoft Edge browser in line with Maturity Level One, they allowed uncontrolled use of other browsers such as Google Chrome and Mozilla Firefox. If web browser settings are not secured, users can change configurations to bypass security policies which can result in system compromise.

Restrict administrative privileges

Users with administrative privileges can make significant changes to systems and applications, bypass security settings and access, modify or delete information.

Restricting administrative privileges introduces guard rails to prevent accidental or malicious access or changes to systems, system settings and information.

[11] Internet Explorer 11 was the final version of browser retired in June 2022.

None of the 10 entities adequately restricted administrative privileges to achieve Maturity Level One. We found common weaknesses, including:

- Privileged administrator accounts were not prevented from accessing the internet, email and web services. To minimise the risk of privileged account takeover, these accounts should not have access to internet-facing services.
- A lack of separate privileged and non-privileged operating environments for administrators.[12]

Multi-factor authentication

Multi-factor authentication (MFA) makes it harder for threat actors to compromise accounts. It requires users to verify their identity by using two or more different factors including:

- something a user knows (such as a PIN or password)
- something a user has (such as a token or an authenticator)
- something a user is (such as a fingerprint or other biometric method).

None of the entities achieved Maturity Level One in this control. While a number of entities had MFA for some systems, they were still in the process of enabling MFA for their remaining systems and all staff. Entities were also in the process of implementing MFA for their internet facing services accessed by non-organisational users (i.e. members of the public).

Regular backups

Regular backups allow for the timely and efficient recovery of system configurations and information in line with business expectations after a disruption.

Backups require systematic testing to ensure they are reliable and must be stored securely to prevent unauthorised changes.

Entities performed better in this control compared to the other controls. Four entities achieved Maturity Level One or higher:

- two entities achieved Maturity Level One
- one entity achieved Maturity Level Two
- one entity achieved Maturity Level Three.

The most common weakness we found was entities not testing the restoration of their backups as part of coordinated disaster recovery exercises. In some instances, backups of important data, software and configuration settings were not in accordance with entities' own business continuity requirements.

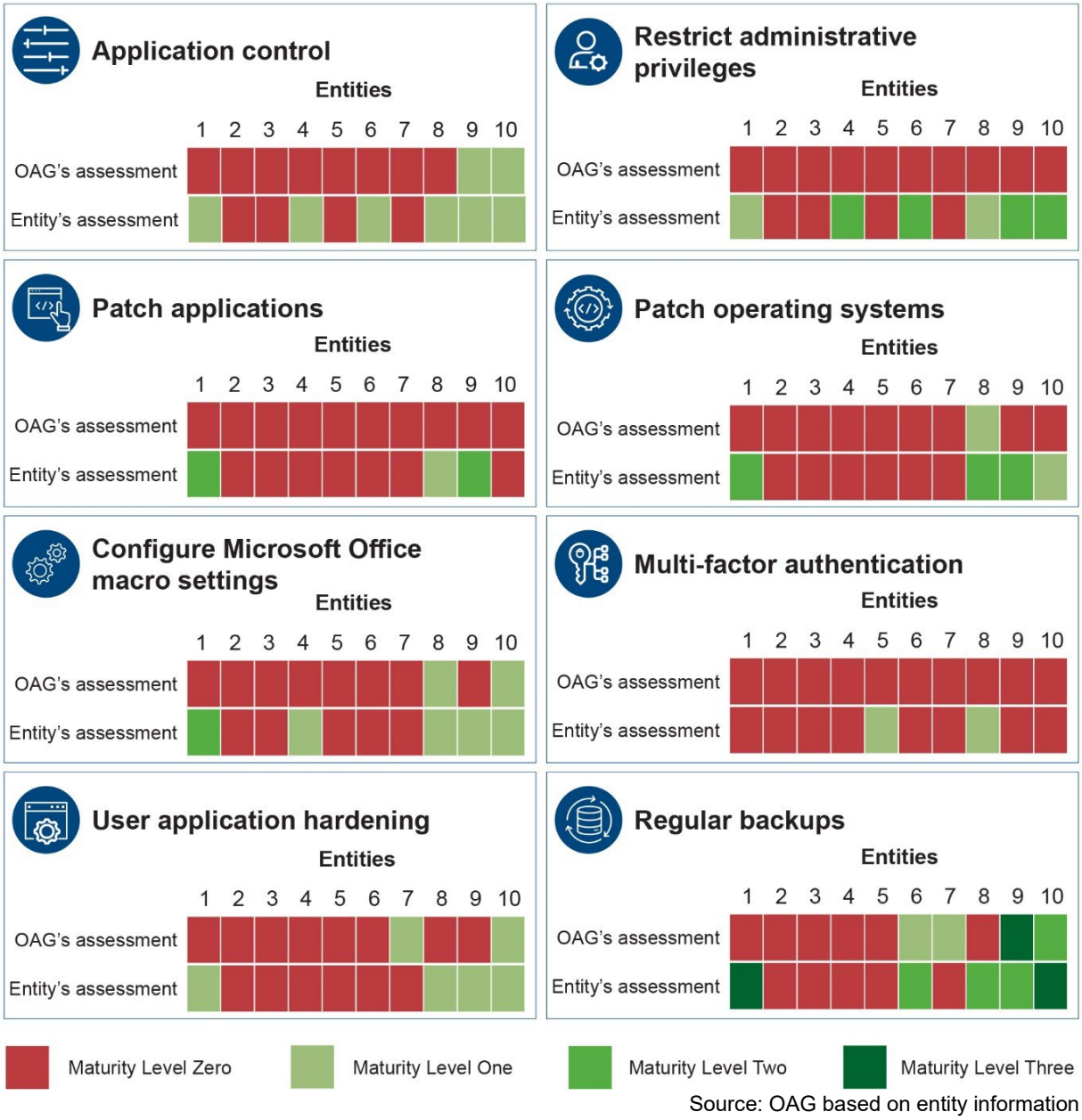
[12] While challenging to implement, separate physical workstations for privileged tasks provide increased security.

Most entities did not have an accurate understanding of their Essential Eight controls maturity

Essential Eight controls at seven entities were not as mature as they had self-assessed and reported to the DGov (Figure 6). If entities do not have a clear understanding of their control maturity they may remain unnecessarily vulnerable to cyber security threats.

Our comparison of entities' self-assessment to our assessments found not all entities had an accurate understanding of their control design or adequately test the effectiveness of controls implementation before completing their self-assessments. This led to incorrect reporting of their maturity levels.

We found three entities accurately assessed their control maturity, one of these has since improved its maturity in two controls. Entities self-assessments were reasonably accurate where they used DGov's preferred third party to confirm their 2022 annual self-assessments prior to submission.



Source: OAG based on entity information

Figure 6: Comparison of entities' self-assessments to our assessments in each control

It is important that entities' self-assessments accurately inform government of the State's cyber risk exposure. The self-assessments are used by DGov to inform sector wide governance and collaboration efforts, such as the Cyber Security Working Group, and to benchmark the sector against other Australian jurisdictions that have adopted the Essential Eight.

The following case studies provide examples of self-assessment questions and entity responses that overstated maturity levels in reporting to DGov.

Case study 1: Entity overstated its maturity for application control

The self-assessment question asked:

> **Q:** Is execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets prevented from within the standard user profiles and temporary folders used by operating system, web browsers and email clients?

The entity self-assessed as having implemented the control at Maturity Level One. The entity's response stated:

> **A:** Workstation and servers.

OAG assessment: We found the entity had only partially implemented the control and did not meet Maturity Level One. While some executables were prevented and controlled, we could run various scripts from user profiles and temporary folders.

Case study 2: Entity overstated its maturity for patch applications

The self-assessment question asked:

> **Q:** How soon are patches, updates or vendor mitigations for security vulnerabilities in other applications (such as Java, SQL, .NET, 7Zip) applied?

The entity self-assessed as having implemented the control at Maturity Level Two. The entity's response stated:

> **A:** Within two weeks.

OAG assessment: Maturity Level One requires mitigation of vulnerabilities on internet facing servers within two weeks, or within 48 hours if an exploit exists. Our assessment found this entity's patching cycle was less frequent (i.e. monthly), and it did not patch vulnerabilities within two weeks. We also identified many unpatched application vulnerabilities on its internet facing servers, some had known exploits for which mitigations had been released five years before.

Case study 3: Entity overstated its maturity for configured Microsoft Office macro settings

The self-assessment question asked:

> **Q:** Are Microsoft Office macros disabled for users that do not have a demonstrated business requirement?

The entity's response stated:

> **A:** Yes.

The self-assessment question also asked:

> **Q:** Are Microsoft Office macros in files originating from the internet blocked?

The entity's response stated:

> **A:** Yes.

OAG assessment: The entity self-assessed as having implemented the control at Maturity Level Two. We found the entity was at Maturity Level Zero as all users could execute macros including those originating from the internet.

The following case study provides an example of one entity that had improved its maturity since reporting to DGov.

Case study 4: Entity had improved its maturity for regular backups since completing its self-assessment

The self-assessment question asked:

> **Q:** Is the restoration of systems, software and important data from backups tested in a coordinated manner as a part of the disaster recovery exercise?

The entity self-assessed as having implemented the control at Maturity Level Zero. The entity's response stated:

> **A:** No, the disaster recovery exercise does not include backup recovery.

OAG assessment: We found the entity had improved its practices as disaster recovery plans and exercises now include recovery testing. The entity met Maturity Level One for regular backups.

Recommendations

1. The Office of Digital Government should continue to support entities implementing Essential Eight controls through reviewing its tools and guidance, and increasing entities' awareness of ACSC maturity levels criteria and assessments tools.
2. Entities should:
    a. continue to implement the Essential Eight controls to meet the WA Government objective of achieving Maturity Level One
    b. test control effectiveness prior to completing self-assessments for DGov
    c. engage and collaborate with the ACSC through its partnership program.

Response from entities

All entities agreed with our assessments of their Essential Eight maturity and advised us they intend to implement Essential Eight controls to at least Maturity Level One.

Response from Office of Digital Government

The Office of Digital Government (DGov) has been working closely with WA Government entities to improve their overall cyber security posture. One of the priority areas for DGov has been to assist agencies implement the Australian Cyber Security Centre's (ACSC) Essential Eight Controls to Maturity Level One.

Since reporting began in 2022, agencies have made substantial progress to understand their cyber security posture and commenced planning and implementing cyber security controls. It is important to highlight that implementing the ACSC's Essential Eight provides baseline protection against currently observed common cyber security threats, however, this should not be used in isolation from broader cyber risk management activities. DGov's focus has been on strengthening cyber security maturity across the WA Government to ensure that it is much harder for adversaries to compromise systems.

DGov are aware of the issues impacting the robustness of self-assessments. We also note that this has been a persistent challenge in other Australian jurisdictions, who also rely on self-assessment reporting. A relevant example is to be found in the observations made in relation to Commonwealth Government entities in Report 497 Inquiry into Commonwealth Financial Statements 2021-22 presented to the Australian Parliament s Joint Committee of Public Accounts and Audit.

In response to emerging issues regarding the robustness of entity self-assessments, DGov has already implemented a four-point plan to improve the accuracy of those assessments comprised of:

- **TAFE Cyber Training** - since September 2023, 70 public sector staff from 49 WA government entities have attended the TAFEcyber Essential Eight assessor course. The course is designed to improve agencies assessment skills and understanding of the Essential Eight controls. DGov supported this training by providing $80,000 to fund agency attendees on the courses.
- **Verification Tool Review** - DGov has assessed multiple cyber security tools to assist agencies with their assessments of Essential Eight controls and provided guidance on best practice methods to apply the tool within their respective environments. A Vulnerability Scanning Service has been established to assist agencies map their Essential Eight compliance.
- **Reporting and Guidance Review** - following the 2022 Annual Implementation Report (AIR), DGov has incorporated further guidance within the current 2023 AIR Assessment templates to enable agencies to better assess the effectiveness of controls in their environment.
- **Independent Essential Eight Verification Assessments** - DGov has engaged an external supplier to provide agencies with the opportunity to undertake an independent assessment of their AIR to provide additional assurance to agencies.

DGov will continue to conduct a review after each AIR period to determine what further measures can be taken to improve the AIR process.

Audit focus and scope

The audit objective was to assess the progress made by a selection of 10 State government entities to implement the Australian Signals Directorate's Essential Eight controls to determine their current maturity level.

In undertaking the audit we:

- engaged closely with audited entities and reviewed their policies and procedures
- reviewed DGov and ACSC guidance and tools
- assessed entities' security controls and maturity using the ACSC Essential Eight Assessment Guide and tools, and provided them with our assessment. This included running executables, attempting to change security configurations, accessing sites with web advertisements and accessing websites through Internet Explorer 11
- compared each entities' 2022 self-assessment provided to the DGov against our own assessment of their maturity.

This was an independent audit conducted under the *Auditor General Act 2006* and arising from our information systems functions. We complied with the independence and other ethical requirements related to assurance engagements. The approximate cost of undertaking the audit and reporting was $165,000.

Appendix 1: Essential Eight maturity level requirements for November 2022 self-assessments

Application control

Maturity Level One	Maturity Level Two *builds from Maturity Level One with additional requirements*	Maturity Level Three *builds from Maturity Level Two with additional requirements*
The execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets is prevented on workstations from within standard user profiles and temporary folders used by the operating system, web browsers and email clients.	**Application control is implemented on workstations and internet-facing servers** to restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets **to an organisation-approved set.**	Application control is implemented on workstations and **servers** to restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets **and drivers** to an organisation-approved set.
	Allowed and blocked executions on workstations and internet-facing servers are logged.	Allowed and blocked executions on workstations and **servers** are **centrally** logged **and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.**
		Microsoft's 'recommended block rules' are implemented.
		Microsoft's 'recommended driver block rules' are implemented.
		Application control rulesets are validated on an annual or more frequent basis.

Source: OAG based on ACSC information

Patch applications

Maturity Level One	Maturity Level Two *builds from Maturity Level One with additional requirements*	Maturity Level Three *builds from Maturity Level Two with additional requirements*
Patches, updates or vendor mitigations for security vulnerabilities in internet- facing services are applied within two weeks of release, or within 48 hours if an exploit exists.	Same as Maturity Level One.	Same as Maturity Level One.
Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within **one month** of release.	Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within **two weeks** of release.	Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within **two weeks** of release, or within **48 hours if an exploit exists**.
A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services.	Same as Maturity Level One.	Same as Maturity Level One.
A vulnerability scanner is used **at least fortnightly** to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.	A vulnerability scanner is used **at least weekly** to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.	Same as Maturity Level Two.
Internet-facing services, office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.	Same as Maturity Level One.	**Applications** that are no longer supported by vendors are removed.
	Patches, updates or vendor mitigations for security vulnerabilities in other applications are applied within one month.	Same as Maturity Level Two.
	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in other applications.	Same as Maturity Level Two.

Source: OAG based on ACSC information

Patch operating systems

Maturity Level One	Maturity Level Two *builds from Maturity Level One with additional requirements*	Maturity Level Three *builds from Maturity Level Two with additional requirements*
Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists.	Same as Maturity Level One.	Same as Maturity Level One.
Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within one month of release.	Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are **applied within two weeks of release**.	Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within two weeks of release, **or within 48 hours if an exploit exists.**
A vulnerability scanner is used at least daily to identify missing patches for security vulnerabilities in operating systems of internet-facing services.	Same as Maturity Level One.	Same as Maturity Level One.
A vulnerability scanner is used at least fortnightly to identify missing patches for vulnerabilities in operating systems of workstations, servers and network devices.	A vulnerability scanner is used **at least weekly** to identify missing patches for security vulnerabilities in operating systems of workstations, servers and network devices.	Same as Maturity Level Two.
Operating systems that are no longer supported by vendors are replaced.	Same as Maturity Level One.	Same as Maturity Level One.
		The latest release, or the previous release, of operating systems are used for workstations, servers and network devices.

Source: OAG based on ACSC information

Configure Microsoft Office macro settings

Maturity Level One	Maturity Level Two *builds from Maturity Level One with additional requirements*	Maturity Level Three *builds from Maturity Level Two with additional requirements*
Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.	Same as Maturity Level One.	Same as Maturity Level One.
Microsoft Office macros in files originating from the internet are blocked.	Same as Maturity Level One.	Same as Maturity Level One.
Microsoft Office macro antivirus scanning is enabled.	Same as Maturity Level One.	Same as Maturity Level One.
Microsoft Office macro security settings cannot be changed by users.	Same as Maturity Level One.	Same as Maturity Level One.
	Microsoft Office macros are blocked from making Win32 API calls.	Same as Maturity Level Two.
	Allowed and blocked Microsoft Office macro execution events are logged.	Allowed and blocked Microsoft Office macro executions are **centrally** logged **and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.**
		Only Microsoft Office macros running from within a sandboxed environment, a Trusted Location or that are digitally signed by a trusted publisher are allowed to execute.
		Only privileged users responsible for validating that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations.
		Microsoft Office macros digitally signed by an untrusted publisher cannot be enabled via the Message Bar or Backstage View.
		Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis.

Source: OAG based on ACSC information

User application hardening

Maturity Level One	Maturity Level Two *builds from Maturity Level One with additional requirements*	Maturity Level Three *builds from Maturity Level Two with additional requirements*
Web browsers do not process Java from the internet.	Same as Maturity Level One.	Same as Maturity Level One.
Web browsers do not process web advertisements from the internet.	Same as Maturity Level One.	Same as Maturity Level One.
Internet Explorer 11 does not process content from the internet.	Same as Maturity Level One.	Internet Explorer 11 is **disabled or removed.**
Web browser security settings cannot be changed by users.	Web browser, **Microsoft Office and PDF software** security settings cannot be changed by users.	Same as Maturity Level Two.
	Microsoft Office is blocked from creating child processes.	Same as Maturity Level Two.
	Microsoft Office is blocked from creating executable content.	Same as Maturity Level Two.
	Microsoft Office is blocked from injecting code into other processes.	Same as Maturity Level Two.
	Microsoft Office is configured to prevent activation of OLE packages.	Same as Maturity Level Two.
	PDF software is blocked from creating child processes.	Same as Maturity Level Two.
	ACSC or vendor hardening guidance for web browsers, Microsoft Office and PDF software is implemented.	Same as Maturity Level Two.
	Blocked PowerShell script executions are logged.	Blocked PowerShell script executions are **centrally** logged **and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.**
		.NET Framework 3.5 (including .NET 2.0 and 3.0) is disabled or removed.
		Windows PowerShell 2.0 is disabled or removed.
		PowerShell is configured to use Constrained Language Mode.

Source: OAG based on ACSC information

Restrict administrative privileges

Maturity Level One	Maturity Level Two *builds from Maturity Level One with additional requirements*	Maturity Level Three *builds from Maturity Level Two with additional requirements*
Requests for privileged access to systems and applications are validated when first requested.	Privileged access to systems, applications and information is validated when first requested **and revalidated on an annual or more frequent basis.**	Same as Maturity Level Two.
Privileged accounts are prevented from accessing the internet, email and web services.	Same as Maturity Level One.	Privileged accounts and **service accounts** are prevented from accessing the internet, email and web services.
Privileged users use separate privileged and unprivileged operating environments.	Same as Maturity Level One.	Same as Maturity Level One.
Unprivileged accounts cannot logon to privileged operating environments.	Same as Maturity Level One.	Same as Maturity Level One.
Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	Same as Maturity Level One.	Same as Maturity Level One.
	Privileged access to systems and applications is automatically disabled after 12 months unless revalidated.	Same as Maturity Level Two.
	Privileged access to systems and applications is automatically disabled after 45 days of inactivity.	Same as Maturity Level Two.
	Privileged operating environments are not virtualised within unprivileged operating environments.	Same as Maturity Level Two.
	Administrative activities are conducted through jump servers.	Same as Maturity Level Two.
	Credentials for local administrator and service accounts are unique, unpredictable and managed.	Same as Maturity Level Two.
	Use of privileged access is logged.	Use of privileged access is **centrally** logged **and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.**

Maturity Level One	Maturity Level Two *builds from Maturity Level One with additional requirements*	Maturity Level Three *builds from Maturity Level Two with additional requirements*
	Changes to privileged accounts and groups are logged.	Changes to privileged accounts and groups are **centrally** logged **and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.**
		Windows Defender Credential Guard and Windows Defender Remote Credential Guard are enabled.
		Just-in-time administration is used for administering systems and applications.
		Privileged access to systems and applications is limited to only what is required for users and services to undertake their duties.

Source: OAG based on ACSC information

Multi-factor authentication

Maturity Level One	Maturity Level Two *builds from Maturity Level One with additional requirements*	Maturity Level Three *builds from Maturity Level Two with additional requirements*
Multi-factor authentication is used by an organisation's users when they authenticate to their organisation's internet-facing services.	Same as Maturity Level One.	Same as Maturity Level One.
Multi-factor authentication is used by an organisation's users when they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data.	Same as Maturity Level One.	Same as Maturity Level One.
Multi-factor authentication (where available) is used by an organisation's users when they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data.	Same as Maturity Level One.	Same as Maturity Level One.
Multi-factor authentication is enabled by default for an organisation's non-organisational users (but they can choose to opt out) when they authenticate to an organisation's internet-facing services.	Same as Maturity Level One.	Same as Maturity Level One.
	Multi-factor authentication is used to authenticate privileged users of systems.	Same as Maturity Level Two.
	Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or are.	*Multi-factor authentication **is verifier impersonation resistant** and uses either: something users have and something users know, or something users have that is unlocked by something users know or are.
	Successful and unsuccessful multi-factor authentications are logged.	Successful and unsuccessful multi-factor authentications are **centrally** logged **and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.**
		Multi-factor authentication is used to authenticate users accessing important data repositories.

Source: OAG based on ACSC information

Regular backups

Maturity Level One	Maturity Level Two *builds from Maturity Level One with additional requirements*	Maturity Level Three *builds from Maturity Level Two with additional requirements*
Backups of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business continuity requirements.	Same as Maturity Level One.	Same as Maturity Level One.
Restoration of systems, software and important data from backups is tested in a coordinated manner as part of disaster recovery exercises.	Same as Maturity Level One.	Same as Maturity Level One.
Unprivileged accounts can only access their own backups.	Unprivileged accounts, **and privileged accounts (excluding backup administrators)**, can only access their own backups.	Unprivileged accounts, and privileged accounts (excluding backup administrators), **can't access backups.**
Unprivileged accounts are prevented from modifying or deleting backups.	Unprivileged accounts, **and privileged accounts (excluding backup administrators)**, are prevented from modifying or deleting backups.	Unprivileged accounts, and privileged accounts (excluding backup **break glass accounts**), are prevented from modifying or deleting backups.

Source: OAG based on ACSC information

Auditor General's 2023-24 reports

Number	Title	Date tabled
9	Implementation of the Essential Eight Cyber Security Controls	6 December 2023
8	Electricity Generation and Retail Corporation (Synergy)	8 November 2023
7	Management of the Road Trauma Trust Account	17 October 2023
6	2023 Transparency Report: Major Projects	2 October 2023
5	Triple Zero	22 September 2023
4	Staff Exit Controls for Government Trading Enterprises	13 September 2023
3	Financial Audit Results – Local Government 2021-22	23 August 2023
2	Electricity Generation and Retail Corporation (Synergy)	9 August 2023
1	Requisitioning of COVID-19 Hotels	9 August 2023

Office of the Auditor General
for Western Australia

7th Floor Albert Facey House
469 Wellington Street, Perth

T: 08 6557 7500
E: info@audit.wa.gov.au

www.audit.wa.gov.au

@OAG_WA

Office of the Auditor General
for Western Australia