



Report 25: 2022-23 | 14 June 2023

INFORMATION SYSTEMS APPLICATION AUDIT

Traffic Management System



Office of the Auditor General Western Australia

Audit team:

Aloha Morrissey
Kamran Aslam
Khubaib Gondal
Paul Tilbrook

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.

© 2023 Office of the Auditor General Western Australia.
All rights reserved. This material may be reproduced in whole or in part provided the source is acknowledged.

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

Traffic Management System

Report 25: 2022-23
14 June 2023

This page is intentionally left blank



**THE PRESIDENT
LEGISLATIVE COUNCIL**

**THE SPEAKER
LEGISLATIVE ASSEMBLY**

TRAFFIC MANAGEMENT SYSTEM

This report has been prepared for submission to Parliament under the provisions of section 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 three key applications that form part of Main Roads Western Australia's Traffic Management System: Traffic Control System, Intelligent Transport System and Travel Time System.

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

A handwritten signature in black ink, appearing to be 'C Spencer'.

CAROLINE SPENCER
AUDITOR GENERAL
14 June 2023

Contents

Auditor General's overview.....	5
Introduction.....	6
Background.....	6
Conclusion	7
Findings.....	8
TMS network and software security was not well managed	8
Weak access controls increase the risk of unauthorised access	9
Physical security of roadside traffic devices needs improvement	9
MRWA's use of monitoring devices on local roads is not permitted and information collected is stored for too long	9
System backups were not frequent enough to meet recovery policy requirements	10
Vendor contract management was inadequate.....	10
Recommendations.....	11
Response from Main Roads WA.....	13
Response from the WA Police Force	14
Audit focus and scope	15

Auditor General's overview

Traffic management is essential to ensure the safe and efficient movement of people and freight across WA's road network.

This audit looked at Main Roads Western Australia's (MRWA) key applications that form part of its Traffic Management System (TMS), to gain assurance that traffic operations are adequately supported.

We found that TMS supports MRWA's traffic management operations. However, MRWA partly protects the TMS and needs to improve security controls to minimise the risk of the system compromise and disruption to traffic operations. Pleasingly, MRWA had started many projects to lift their cyber security maturity across the TMS network.

In addition, despite being aware they are not permitted to, MRWA has continued to collect anonymous data from local road users under the Surveillance Devices Regulations 1999. We have recommended they comply with the Regulations.



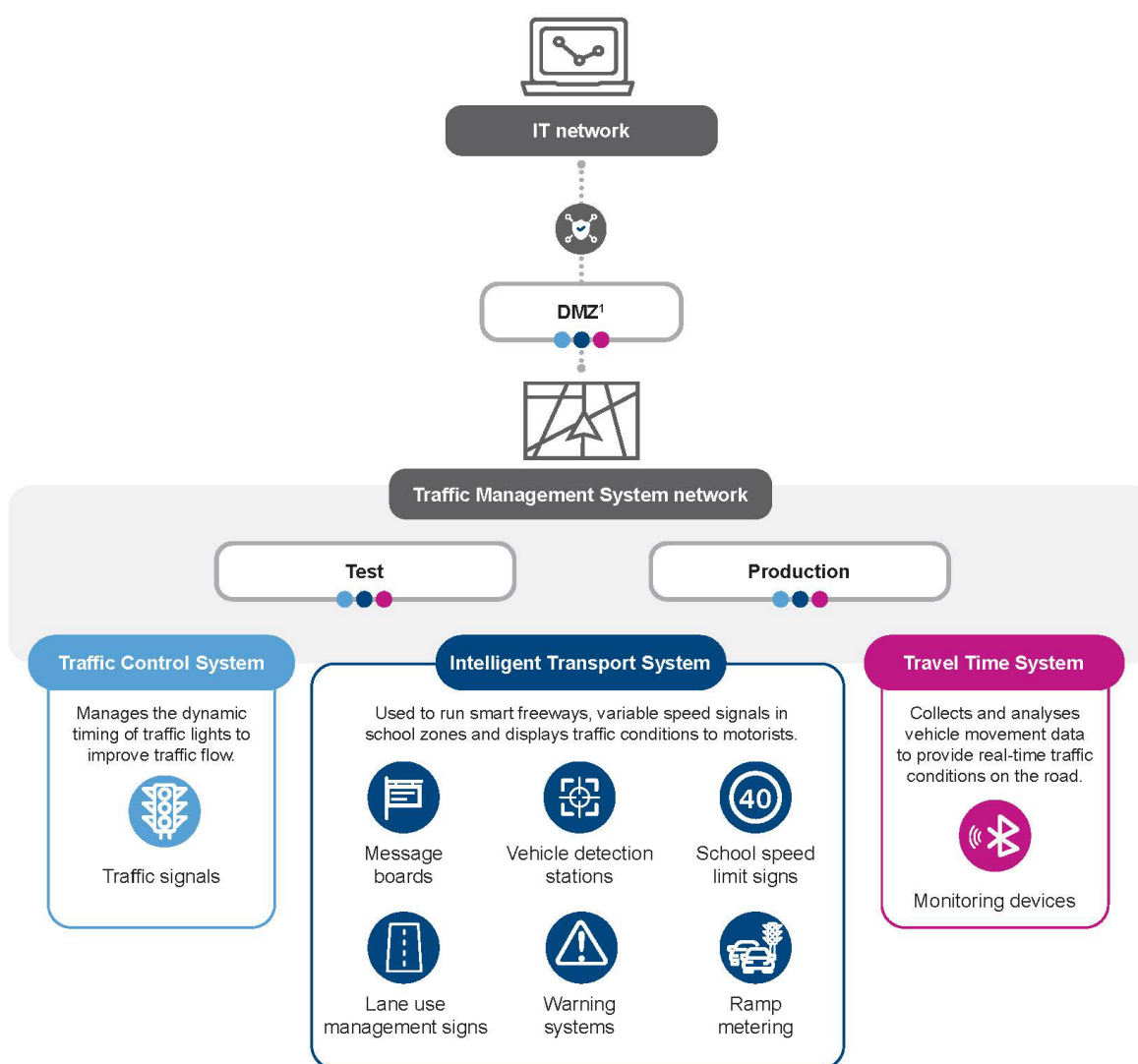
Introduction

This audit assessed the three key applications that form part of Main Roads Western Australia's (MRWA) Traffic Management System (TMS): Traffic Control System, Intelligent Transport System and Travel Time System.

We reviewed if the availability and integrity of MRWA's traffic operations were adequately supported by the TMS. We also reviewed if the confidentiality of information generated by and stored in the three applications was appropriate.

Background

MRWA uses the TMS to facilitate the safe movement of people and freight across WA's road network. An overview of the TMS and its related applications is shown in Figure 1.



Source: OAG based on MRWA information

Figure 1: Overview of the TMS

¹ A demilitarised zone (DMZ) is the separation of a network to prevent direct access to critical systems.

In addition to traffic control operations, information from TMS is used by MRWA to:

- liaise with State and local government entities, and other traffic management organisations to monitor and manage traffic congestion, incidents and planned events
- provide road users and media with real-time and scheduled information about incidents or events that may affect a journey
- report against internal key performance indicators (such as vehicle kilometres travelled and speed) using traffic signal, speed, and volume
- measure its response to incidents on smart freeways.

Key information from TMS that is shared with other entities includes traffic incidents, daily traffic data, road closures, crash information and travel maps of the road network and signs.

Conclusion

The TMS is critical to MRWA's delivery of traffic operations across WA's road network. While MRWA has processes in place to partly protect the TMS system from unauthorised access and use, we identified weaknesses that could be used to compromise the system and, in so doing, disrupt traffic operations.

Security vulnerabilities and weak database and access controls put TMS availability and integrity at risk. MRWA also did not verify or monitor TMS configuration changes to devices such as traffic signals. However, safety controls such as default speed limits are built into the system to reduce the risk of outages and road accidents. Further, MRWA had not established adequate contractual arrangements with all TMS vendors and did not effectively monitor vendor performance against agreed service level. MRWA has projects underway to uplift the cyber security of its TMS network, which will also help address these audit findings.

We also found MRWA's use of vehicle monitoring devices² on local roads is not permitted by the Surveillance Devices Regulations 1999. These devices collect anonymous data from vehicles on highways, main roads and local roads for MRWA to monitor road congestion and traffic flow. However, the Regulations do not allow the use of these devices on local roads. MRWA is working with key stakeholders to draft changes to the Regulations.
















² These are described as tracking device in the *Surveillance Devices Act 1998*, which is any instrument, apparatus, equipment or other device capable of being used to determine the geographical location of a person or object.


Findings

TMS network and software security was not well managed

TMS and related systems are appropriately segregated from MRWA’s IT network and further segregated across physical locations and field devices. However, we found the following gaps which weaken the security of the TMS network:

- **Misconfigurations allow security controls to be bypassed** – misconfigurations in the TMS test network³ mean unapproved devices can bypass controls and access key production servers and field devices including traffic signal controllers, message boards and surveillance devices. MRWA informed us they have a project underway to address these risks.
- **Software vulnerabilities could be exploited** – MRWA’s monthly vulnerability scans do not cover the majority of the TMS network such as key application servers and workstations. Understanding vulnerabilities in critical systems is key to being able to fix them promptly. We also found legacy and unsupported software in the TMS network. Vulnerabilities in unsupported software could be exploited to compromise traffic operations.
- **Removable media and malware controls were inadequate** – MRWA did not enforce its removable media policy to restrict the use of personal media storage devices, such as USB drives, in the TMS network or have controls in place to block malicious code embedded in documents. These weaknesses can allow the spread of malware capable of disrupting traffic operations.
- **Database⁴ security was weak** – the three TMS applications’ databases had inadequate security controls (Table 1) to protect the integrity of information. A compromise could result in loss of accurate and complete information for decision-making and disrupt MRWA’s operations.

Database controls	Application 1 database	Application 2 database	Application 3 database
Supported software			
Patch management			
Strong passwords			
Access and privilege management			
Execution of operating system commands			

 Effective  Ineffective

Source: OAG

Table 1: Control weaknesses in TMS databases

³ Test environments are used to trial systems and configurations before implementing in production systems.

⁴ Databases store information generated and processed by systems.

Weak access controls increase the risk of unauthorised access

- **Privileged activities were not monitored** – a high number of accounts were granted privileged access to one of the TMS applications, which MRWA promptly addressed when we notified it of the issue. In addition, MRWA did not have a mechanism to log and monitor key events in the TMS network including access activity, use of privileges and configuration changes to traffic signals, speed limit signs and lane management systems. Without monitoring, MRWA will not detect unauthorised access or malicious activity promptly. In addition, if the logging process is not adequate it may not provide suitable evidence to support forensic or internal investigations.
- **MRWA had not reviewed dormant network accounts** – we identified seven contractor and eight employee accounts that had not been used for over nine months and had not been disabled from the network. Dormant accounts could be used for malicious purposes. To address the risk of excessive dormant accounts, MRWA's access process requires all contractor accounts to be created with an expiry date, but we identified a small number of contractor accounts without this.
- **Weak password requirements** – one TMS application had weak password configuration which did not meet MRWA's password policy, increasing the risk of compromise.

Physical security of roadside traffic devices needs improvement

MRWA does not appropriately safeguard the universal keys to access and lock roadside cabinets which house device controllers and communication equipment for the TMS. We found six individuals, including contractors and third-party service providers, had been issued multiple keys. There was no record to show why multiple keys were issued and if keys were returned when staff or contractors stopped working for MRWA. While electronic alerts are generated when a cabinet is opened, these alerts are not reviewed to determine if the cabinet was accessed for legitimate reasons. Without appropriate physical protection, there is an increased risk of compromise to the communication equipment, power supply and traffic signal devices housed in these cabinets.

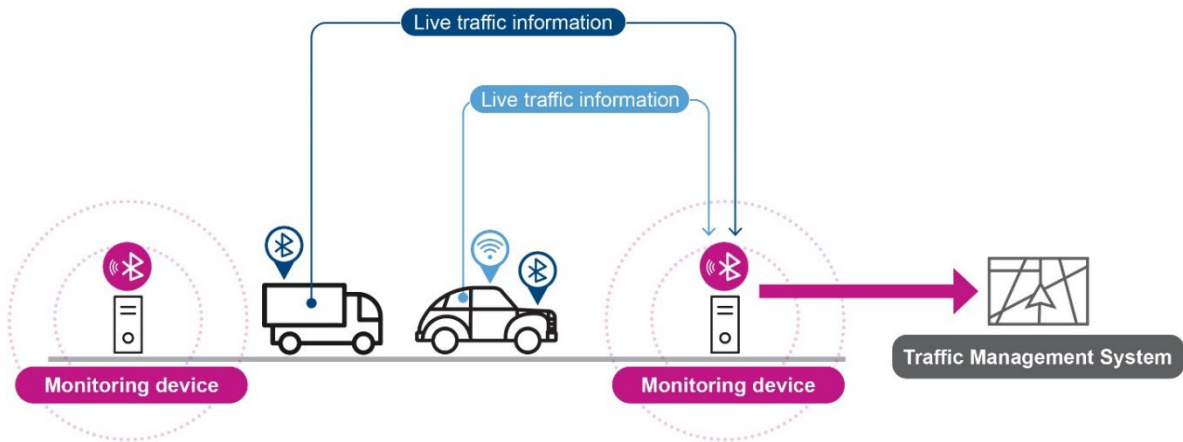
MRWA's use of monitoring devices on local roads is not permitted and information collected is stored for too long

MRWA has known since the Surveillance Devices Regulations 1999 (Regulations) were updated in 2016 that vehicle monitoring devices were only permitted on highways and main roads. Despite this, MRWA uses over 180 devices on local roads to monitor traffic congestion. MRWA has consulted widely with key stakeholders including State and local government entities since as early as 2020 to draft changes to the Regulations to permit the use of monitoring devices on local roads. Amendments to the Regulations were still pending at the time of our audit.

We found Media Access Control (MAC⁵) addresses collected by the vehicle monitoring devices were stored by TMS for 30 days and not the one day MRWA expected. MRWA told us it has worked with the application vendor to limit data storage to one day.

⁵ MAC addresses are a distinct attribute used to identify electronic devices. For example phones, laptops and navigation systems have a unique address associated to them.

MRWA collects MAC addresses from road traveller devices such as car infotainment systems and mobile phones, and uses them to calculate travel times between locations. While MAC addresses are not considered personal information on their own, they can be used to track individuals. We found no instances of MRWA doing this.



Source: OAG

Figure 2: Monitoring devices used to calculate travel time

System backups were not frequent enough to meet recovery policy requirements

MRWA's backups did not meet its recovery objectives for TMS. MRWA's policy sets a maximum data loss of eight hours, but MRWA only backed up the system every 24 hours and some servers were not backed up at all. In the event of a TMS failure, MRWA may not have all the information it needs for decision-making. MRWA told us it will update its recovery objectives to address the gap.

Vendor contract management was inadequate

MRWA did not have adequate contractual arrangements with its three TMS vendors. The contract with one vendor required an escrow⁶ agreement which had not been developed and implemented since 2013. MRWA had not established documented contracts with the other two vendors. Without documented arrangements MRWA may not receive expected services to effectively operate TMS and the traffic network. MRWA told us the contract with the first vendor has been strengthened, and it plans to establish formal contracts with the other two vendors.

Additionally, MRWA did not monitor TMS vendor performance against agreed service levels. For one TMS application we found 18 of the 38 service tickets raised in the last six months required resolution in seven days, but were resolved in between 45 and 155 days, and some were still unresolved at the time of our audit. MRWA was not aware of this underperformance until our audit. For the other two TMS applications, resolution reports lacked information for MRWA to measure and assess if service levels were achieved.

⁶A software escrow helps protect all parties involved in a software license by having a neutral third party (escrow agent) hold source code, data and documentation.

Recommendations

MRWA should:

1. [comply with the Surveillance Devices Regulations 1999 around the use of vehicle monitoring devices on local roads](#)

Implementation timeframe: Q3 2023

Entity response:

Main Roads is progressing, in coordination with Western Australia Police Force (WAPOL) and in consultation with the Western Australian Local Government Association (WALGA), a proposed amendment to Surveillance Devices Regulations 1999 (the Regulations) for the collection of anonymised travel time data from Bluetooth detectors installed on local roads in addition to highways and main roads currently covered under the Regulations. Following continued liaison with WAPOL, this amendment to the Regulations will be aligned with relevant amendments to the *Main Roads Act 1930* as part of the Main Roads Amendment Bill 2023.

2. [review and enhance security controls to address weaknesses in the TMS network](#)

Implementation timeframe: June 2024

Entity response:

Previously the upgrades to the Traffic Control Systems (TCS) environment have been driven with the application updates from the vendors. Main Roads has been taking a more active role in the management of the TCS environment with the roles and responsibilities between the stakeholders now clearly defined. Main Roads will work with the vendors to update the databases and ensure all vendors provide software that runs on supported platforms.

3. [promptly remediate software vulnerabilities affecting TMS systems, to minimise the risk of compromise through attacks that exploit these vulnerabilities](#)

Implementation timeframe: June 2024

Entity response:

Previously the upgrades to the Traffic Control Systems (TCS) environment have been driven with the application updates from the vendors. Main Roads has been taking a more active role in the management of the TCS environment with the roles and responsibilities between the stakeholders now clearly defined. Main Roads will work with the vendors to update the databases and ensure all vendors provide software that runs on supported platforms.

4. [improve access controls to TMS applications and the network to ensure only authorised users have access](#)

Implementation timeframe: June 2023

Entity response:

Main Roads Information Communications Technology (ICT) team has been taking a more active role in the management of the TCS environment, this includes alignment of cyber security framework with the user access management controls being completed during the audit.

5. patch out-of-date databases, disable unused database functions and use the principle of least privilege to grant permissions

Implementation timeframe: August 2023

Entity response:

Main Roads will work with the vendors to update the databases and ensure all vendors provide software that runs on supported platforms.

Main Roads has removed privileges access from accounts that no longer require it. A more robust review process will be put in place to ensure privileged access is managed for Traffic Management Systems.

6. develop appropriate key management procedures and physical controls to safeguard roadside cabinets and monitor access

Implementation timeframe: October 2023

Entity response:

Main Roads will develop a more robust key management procedure and integrate door alarms to match with site logs and identify exceptions and any potential unauthorised cabinet access.

7. enhance backup practices to meet its policy objectives

Implementation timeframe: June 2023

Entity response:

Agreed with business application owners to change the Recovery Point Objective (RPO).

8. establish appropriate contracts and mechanisms to manage vendor performance.

Implementation timeframe: December 2023

Entity response:

Main Roads has already put in place a new contract and service level agreement mechanism for vendor 1. Additionally, Main Roads is currently establishing formal contracts with software vendors for the additional 2 vendors referred to in this report (Currently under license agreement with other State government departments). Contracts put in place by Main Roads will ensure national alignment with service level offerings for both applications.

Response from Main Roads WA

Main Roads Western Australia (Main Roads) is committed to improving the mobility of people and the efficiency of freight. The Application Controls Audit of our Traffic Management Systems (TMS) will play an important part in helping us to shape how we continue to build on the significant progress we have made in recent years with the work undertaken in respect to our technology, supplier relationships and people development in response to traffic congestion.

This work to date has centred around increasing capability year on year; getting the right people in place, forensically measuring the Road Network performance through new devices and systems, optimising the performance of the arterial road network and Freeways and selecting the right game changing projects as we reach new levels of maturity, such as Perth's first Smart Freeway together with the development of a World Class Road Network Operations Centre (RNOC) operating 24/7 to support Main Roads transition to real time intelligence led decision making, which supports the customer journey.

The on-going development of our systems to support the operation is guided by our Intelligent Transport Systems (ITS) Master and Delivery Plan with a medium term view to 2030, in order to focus on the right projects and capability.

The outcomes of the TMS audit will play an important part in building on the significant work to date to shape Main Roads response to the implementation and management of ITS both now and into the future to ensure elements such as security controls over the technology and appropriate contract management of vendor systems, align with continuous improvement and best practice.

Main Roads is also committed to continue the work commenced over recent years to improve its cyber security positioning in relation with key activities already underway to implement the following improvements:

- Traffic Control Systems (TCS) resilience program of works.
- Cyber Security Strategy and Framework that encompasses the TCS
- Cyber security function which includes TCSs.
- Supply chain risk analysis and gap analysis for Third Party vendors relating to TCS.
- Cyber security awareness training for Operations.
- Asset management framework to manage end-point protection of roadside technologies.
- Monitoring processes for network traffic.
- Development and implementation of processes to manage accounts with elevated privileges.

Response from the WA Police Force

WA Police Force has carefully reviewed the findings that pertain to the legal use of the monitoring devices. Furthermore, we have been actively pursuing amendments to the regulations that expand upon their usage.

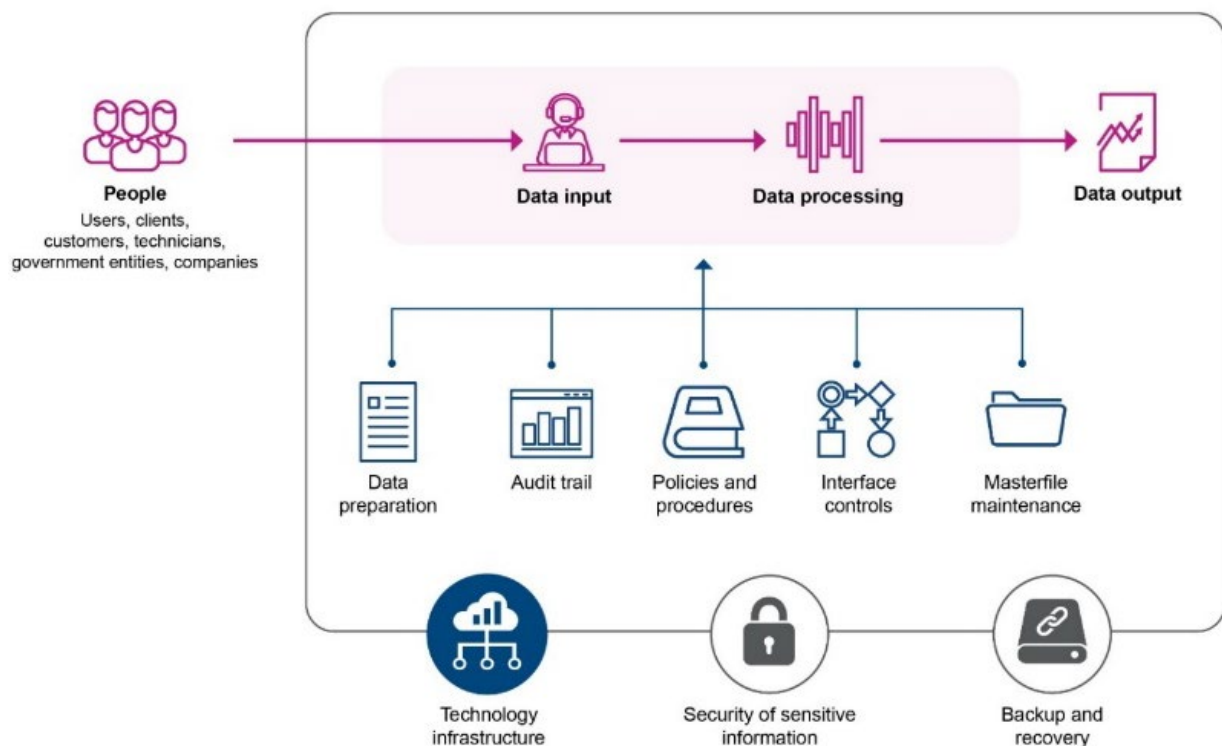
According to the Surveillance Devices Regulations 1999 (the Regulations), the MRWA is currently authorised to monitor traffic exclusively on highways or main roads, as specified in Section 6(1)(da). However, as highlighted in this report, the use of monitoring devices by MRWA on local roads is presently prohibited under the same Regulations. To enable monitoring on local roads, amendments to the Regulations will be necessary.

The WA Police Force is responsible for advancing these changes to the Regulations, and confirm that our Standards and Legal Portfolio have been collaborating with Legal and Insurance Services, MRWA, since early 2020 to draft the required amendments. In December 2022, WAPOL received a formal request from the Director General - Transport, seeking approval for such amendments, which is still pending. Nonetheless, WAPOL confirms that the Western Australia Police Force remains actively engaged with MRWA and the Parliamentary Counsel's Office on this matter.

Audit focus and scope

Each year we review a selection of important software programs (applications) that public sector entities rely on to facilitate their key business processes. Applications help entities perform important routine functions (such as finance, human resources, case management, licensing, billing and service delivery) and those functions that are unique and essential to them. If applications and their related processes are not managed appropriately, stakeholders including the public, may be affected.

Our application controls audits focus on people, process, technology and data. In considering these elements, we follow data from input and processing through to storage, handling and outputs.



Source: OAG

Figure 3: Key elements of focus in our application audits

We review key controls that ensure information is complete, accurately captured, processed and maintained. Failures or weaknesses in these controls can result in loss or inappropriate use or disclosure of information, service delivery delays and disruptions, and increase the risk of fraud and financial loss.

Our tests may highlight weaknesses in control design or implementation that increase the risk that an application's process or information may be susceptible to compromise. While our tests are not designed to identify if information has been compromised, we may become aware of instances during an audit.

During this audit we reviewed key TMS controls and processes to obtain reasonable assurance that the applications worked as intended. Our testing was performed between October 2022 and March 2023.

We also shared relevant findings with the WA Police Force as they are responsible for advancing changes to the Regulations, which will allow MRWA to use monitoring devices on local roads.

This was an independent audit, conducted under section 18 of the *Auditor General Act 2006*, and in accordance with Australian Auditing and Assurance Standards. The approximate cost of undertaking the audit and reporting was \$115,000.

Auditor General's 2022-23 reports

Number	Title	Date tabled
24	Security Basics for Protecting Critical Infrastructure from Cyber Threats – Better Practice Guide	14 June 2023
23	Contractor Procurement – Data Led Learnings	14 June 2023
22	Effectiveness of Public School Reviews	24 May 2023
21	Financial Audit Results – State Government 2021-22 – Part 2: COVID-19 Impacts	3 May 2023
20	Regulation of Air-handling and Water Systems	21 April 2023
19	Information Systems Audit – Local Government 2021-22	29 March 2023
18	Opinions on Ministerial Notifications – Tourism WA's Campaign Expenditure	27 March 2023
17	Information Systems Audit – State Government 2021-22	22 March 2023
16	Opinions on Ministerial Notifications – Triennial Reports for Griffin Coal and Premier Coal	22 March 2023
15	Opinion on Ministerial Notification – Stamp Duty on the Landgate Building, Midland	8 March 2023
14	Administration of the Perth Parking Levy	16 February 2023
13	Funding of Volunteer Emergency and Fire Services	22 December 2022
12	Financial Audit Results – State Government 2021-22	22 December 2022
11	Compliance with Mining Environmental Conditions	20 December 2022
10	Regulation of Commercial Fishing	7 December 2022
9	Management of Long Stay Patients in Public Hospitals	16 November 2022
8	Forensic Audit Results 2022	16 November 2022
7	Opinion on Ministerial Notification – Tom Price Hospital Redevelopment and Meekatharra Health Centre Business Cases	2 November 2022
6	Compliance Frameworks for Anti-Money Laundering and Counter-Terrorism Financing Obligations	19 October 2022
5	Financial Audit Results – Local Government 2020-21	17 August 2022
4	Payments to Subcontractors Working on State Government Construction Projects	11 August 2022
3	Public Trustee's Administration of Trusts and Deceased Estates	10 August 2022
2	Financial Audit Results – Universities and TAFEs 2021	21 July 2022
1	Opinion on Ministerial Notification – Wooroloo Bushfire Inquiry	18 July 2022

**Office of the Auditor General
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