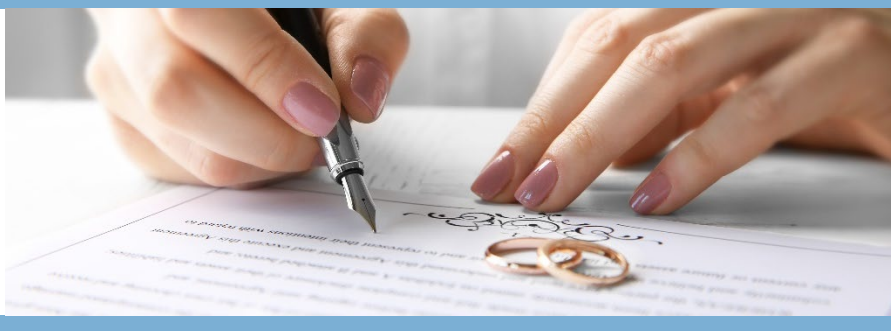
Western Australian
Auditor General's Report



# Western Australian Registry System – Application Controls Audit

Report 9: 2020-21
26 November 2020

**Office of the Auditor General**
**Western Australia**

**Audit team:**
Jordan Langford-Smith
Aloha Morrissey
Kamran Aslam
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.



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

# Western Australian Registry System – Application Controls Audit

Report 9: 2020-21
November 2020

**THE PRESIDENT**
**LEGISLATIVE COUNCIL**

**THE SPEAKER**
**LEGISLATIVE ASSEMBLY**

## WESTERN AUSTRALIAN REGISTRY SYSTEM – APPLICATION CONTROLS AUDIT

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.

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

CAROLINE SPENCER
AUDITOR GENERAL
26 November 2020

# Contents

# Auditor General's overview

Our eleventh annual Information Systems Audit Report was tabled in Parliament on 15 May 2019. The report contained the results of the 2018 annual cycle of information systems audits. These included findings from our audit of key business applications at 4 public sector entities, as well as the results of our general computer controls and capability assessments.

The following report summarises the results of a further application controls audit that my office performed at the same time, of the Western Australian Registry System, used by the Registry of Births, Deaths and Marriages (a division of the WA Department of Justice).

The results of the audit were so concerning that, in a highly unusual step and in accordance with sections 7(6) and 25(1) of the *Auditor General Act 2006*, I decided not to include the results of this application controls audit in the May 2019 report to Parliament. I considered that publishing the significant findings at that time, when the system vulnerabilities still existed, would not be in the public interest. Instead, I provided my parliamentary oversight committees, the Public Accounts Committee and Estimates and Financial Operations Committee, as well as relevant Ministers, with briefings and the detailed report in confidence.

My Office frequently finds weaknesses in public sector entities' systems, as reported in my tabled reports. However, the nature of the data in the Western Australian Registry System, and what it can potentially be used for, renders the findings in this report particularly concerning. Knowledge of weaknesses in this system would be of keen interest to those with malicious intent who seek financial or other gains from the alteration or access to foundational identity records of Western Australian citizens. The risk is higher due to other weaknesses in the Department of Justice's broader IT environment, also identified by this Office in previous audits over the years. These have included weak network security, access and vulnerability management controls, which are designed to protect the confidentiality and integrity of sensitive and privileged data. Each are important layers to maintain effective defence against security threats.

Since the 2019 findings were reported to the Department, the Director General has provided me with regular updates on the progress of work to address the shortcomings, and my Office has since verified key aspects of actions implemented to address the weaknesses. It was important to address these aspects before public reporting, else it may have exposed a critical system and dataset to deliberate harm.

The recommendations to address the findings in this report may be relevant to other public sector operations. Ensuring entities implement and enforce good security practices and regularly test them should be a focus and key responsibility for all executive teams, particularly where highly sensitive and valuable data is involved. Continually raising staff awareness, at all levels, of information and cyber security issues is another proven way to embed good practice and security hygiene into everyday operations.

Furthermore, it is important to recognise that outsourcing system development and maintenance to third party vendors, who have access to sensitive data, does not absolve any public sector entity of responsibility for strong data governance. Indeed, an understanding of risks, and capability for monitoring and oversight, are of heightened importance.

# Application controls audits

## Introduction

Applications are software programs that facilitate an organisation's key business processes including finance, human resources, case management, licensing and billing. Applications also enable entities to perform important functions that are unique and essential to them. Applications may affect stakeholders, including the public, if the application and related processes are not managed appropriately.

Each year we review a selection of important applications that entities rely on to deliver services. We focus on the key controls that ensure data is complete, accurately captured, processed and maintained. Failings or weaknesses in these controls have the potential to affect other organisations and the public. Impacts range from delays in service and loss of information, to possible fraudulent activity and financial loss.

## Audit focus and scope

Our audits focus on the systematic processing and handling of data in the following control categories:

1. **Policies and procedures** – are appropriate and support reliable processing of information.
2. **Security of sensitive information** – controls exist to ensure integrity, confidentiality and availability of information at all times.
3. **Data input** – information entered is accurate, complete and authorised.
4. **Backup and recovery** – is appropriate and in place in the event of a disaster.
5. **Data output** – online or hard copy reports are accurate and complete.
6. **Data processing** – information is processed as intended, in an acceptable time.
7. **Segregation of duties** – no staff perform or can perform incompatible duties.
8. **Audit trail** – controls over transaction logs ensure history is accurate and complete.
9. **Masterfile maintenance, interface controls, data preparation** – controls over data preparation, collection and processing of source documents ensure information is accurate, complete and timely before the data reaches the application.

Our testing of the Western Australian Registry System was a point in time assessment. We reviewed a sample of key controls and processes to obtain reasonable assurance that the application worked as intended and that information it contained and reports were reliable, accessible and secure. Our testing may highlight weaknesses in control design or implementation that increase the risk that an application's information may be susceptible to compromise. However, we do not design our tests to determine if information has been compromised.

# WA Registry System – Department of Justice

## Introduction

The Department of Justice's (the Department) Registry of Births, Deaths and Marriages (Registry) uses the Western Australian Registry System (System) to manage information on all births, adoptions, deaths, marriages and change of name records for Western Australia (WA). The System contains valuable records that are used to confirm people's identity. This information, similar to land titles, is foundational to a civil society.

On 15 May 2019, we tabled our *Information Systems Audit Report 2019* in Parliament. While we also reviewed application controls for the System, we did not include these findings in the report because they were so significant that reporting would not be in the public interest.

A follow up audit this year highlighted the Department's improvements and significant work to address the findings from the previous audit. This report summarises the results of both our initial and follow-up audit.

## Conclusion

The System works as intended. It stores and manages registered life events for the people of WA, including births, deaths, marriages and change of name records.

However, our 2019 audit found that the System was not adequately protecting the confidentiality and integrity of information housed within it. Highly confidential and foundational information was at risk of unauthorised access, alteration and disclosure due to inadequate database controls, security vulnerabilities and insufficient monitoring of changes to critical information. Insufficient disaster recovery planning also meant that the System was at risk of not being recovered in a timely manner in the event of a disruptive incident.

The Department has made a number of changes since our initial audit to improve information security. However, more work is needed to fully implement our recommendations, which will help protect the confidentiality and integrity of the sensitive information contained in the System.

## Background

The Registry is a division of the WA Department of Justice. It registers all adoptions, births, deaths, marriages and change of name events in the State in accordance with the requirements of the *Births, Deaths and Marriages Registration Act 1998*. The system records and authorises the creation of foundational identity and other legal documents for citizens.

The System is the application that supports the key business processes of the Registry. It holds records dating back to 1841 when the Registry was first established. A third party vendor developed the System in 2001, and continues to maintain it.

## Findings

### The Department did not know if inappropriate or unauthorised changes were made to information stored in the System

In 2019, we found that the Department did not appropriately monitor access to information, nor changes made.

There were inadequate controls in place to ensure access and changes were appropriate and authorised in the application and the database that stores all of the System information. In particular:

- we found 11 third-party vendor staff had full access to the database and could make changes to information, such as names and life events. The Registry would not know if vendor staff had inappropriately accessed or changed information as there was no logging or auditing of the database
- the application captured changes made to records, but there was no process to alert the Registry of sensitive and high risk transactions. These could include modification of restricted records, access outside business hours or a pattern of failed access attempts. As a result, the Department could not identify unauthorised changes or access to System information in a timely manner.

Our follow-up audit in 2020 identified that the Department has reduced the number of staff with full access to the database and developed a process to monitor key changes made to information in the database. The monitoring process is maturing, though it could be enhanced by having the review performed by an independent officer who does not have administrator access to the database and is fully informed of relevant risks and controls. The Department has also developed a process to alert and monitor access to highly sensitive records in the production, development and test environments.

## The security of electronic records needed improvement

The System contains confidential personal and sensitive information, which is not protected through encryption, nor is it masked in test environments. Security weaknesses we identified in 2019 included:

- **Insecure databases** – there was no data encryption to protect confidential information in the database. This means that information contained in the System could be exposed in the event of a data breach. The Department is now investigating the use of encryption and its impacts on their operations.

  We also found that the password for the system administrator account had not been changed for an extended period and there were a small number of database accounts with weak passwords. Privileged database accounts are the first accounts an attacker will try to compromise in order to gain unauthorised access to information. In our follow-up audit we found that the Department is now enforcing its password standards on all accounts.

- **Unprotected personal data** – confidential information was replicated without obfuscation[1] in the test and development environments, neither of which had effective security controls. Processing and storing confidential information without appropriate levels of protection increases the risk of unintentional and unauthorised disclosure or changes to confidential information.

  In addition, a lack of segregation of duties meant that developers had full access to the test, development and production (live) environments. This weakness could result in inappropriate changes, which could compromise the confidentiality, integrity and availability of the System.

  In 2020, the Department developed a process to receive alerts if sensitive data is accessed in test, development and live environments. While the Department assessed whether it could mask data in test and development environments, it ultimately decided not to. This is because the Department relies heavily on its test environment for business continuity.

[1] Data obfuscation is a technique which copies and conceals sensitive information to protect the privacy in non-production environments. These environments are generally used for testing and development activities.

## Security vulnerabilities were not well managed, leaving the System exposed to attacks

Our 2019 audit found that the System was not adequately protected from the threat of cyber-attacks. Our vulnerability scans on a sample of workstations and key System servers identified a number of vulnerabilities due to unsupported third party applications, misconfigurations and missing security patches. These vulnerabilities were present on the web, database and audit reporting servers across the development, test and production environments. Regular patching and vulnerability scans are important for securing systems.

By contrast, we found that the Department managed patches for operating system software well. Our testing in 2019 of a sample of servers did not identify any significant issues. Timely patching of software reduces the risk of potential attacks.

In our 2020 follow-up audit, we identified that the Department has undertaken significant work to improve its vulnerability management capabilities. It is also addressing long standing vulnerabilities that affect its systems.

## The change of name process could be misused

The following information is needed to validate a change of name application:

- age (18 years or older)
- place of birth
- residency duration in WA
- number of times an applicant has changed name in 12 months
- whether the applicant is a reportable offender, who is required to keep the police informed of their whereabouts and personal details.

We found the System only validates change of name applicants against national offender information for reportable offences such as crimes against children. Other serious offenders, prisoners and parolees could still change their names for wrongful purposes without additional scrutiny.

Only 5 Australian states participate in the system to cross-check change of name applications against name changes made in other states. A team of supervisors check applications against the national Change of Name Search System to confirm the applicant has not changed their name in the past 12 months. However, the search is not as effective as it could be because 3 states and territories do not participate.

The Registry became aware of these limitations in 2011, and has been working towards updating the *Births, Deaths and Marriages Registration Act 1998* to address some of the shortfalls. In 2018, the Births, Deaths and Marriages Registration Amendment (Change of Name) Bill 2018 was introduced in Parliament. The Department advised that the Bill will improve the change of name process and minimise the risk of exploiting the current system for fraudulent, criminal or other wrongful activity.

## The Department does not know if it will be able to recover the System following an incident

The Department does not have an information technology disaster recovery plan that outlines the process to recover the System, including key infrastructure that it is dependent on, following a major incident or disruption. There is an increased risk that the Department will not be able to restore systems to deliver its key services following an incident which could result in significant reputational damage.

## Recommendations

The Department should:

1. continue to strengthen its controls for systems that store sensitive information

   **Response:** Agreed

   **Implementation timeframe:** by June 2021

2. continue to improve its framework to log and monitor key events in the System

   **Response:** Agreed

   **Implementation timeframe:** by June 2021

3. continue to enhance the change of name process to minimise the risk of misuse

   **Response:** Agreed

   **Implementation timeframe:** Legislation currently before Legislative Council

4. regularly review the effectiveness of key controls to protect information in the System

   **Response:** Agreed

   **Implementation timeframe:** by June 2021

5. develop, regularly review and test the information technology disaster recovery plan

   **Response:** Agreed

   **Implementation timeframe:** by June 2021

6. review and enhance the vulnerability management process.

   **Response:** Agreed

   **Implementation timeframe:** by December 2021

## Response from the Department of Justice

The Department of Justice, Registry of Births, Deaths and Marriages (the Registry) welcomes the recommendations from the application controls audit by the Office of the Auditor General (OAG). The integrity, confidentiality and availability of the Western Australian Registry System (WARS) remains a high priority and the audits conducted by the OAG assist the Registry in increasing compliance and governance. The Registry continues to address all recommendations where reasonable and provides the following commentary:

1. The Registry has reduced the number of its database administrators and has developed an audit process to monitor key changes made to information in the database. A project to migrate all SQL 2008 databases to supported platforms continues to enable increased security and logging capabilities and the Registry will continue to investigate additional tools and processes to strengthen controls.
2. The Registry has engaged a Data Integrity Coordinator and commenced an audit process to monitor the access of restricted records across all WARS environments. This audit function is fully documented and the Registry continues to review system administration privileges and access roles.
3. The Registry identified risks associated with the change of name process in 2011 and in 2018 tabled the Births, Deaths and Marriages Registration Amendment (Change of Name) Bill 2018 in Parliament. The Registry is currently awaiting passage of this bill.
4. The Registry now has audit logging in place to monitor key changes made directly to the WARS production database. An audit process has been documented and is carried out by the Data Integrity Coordinator. The use of system deployment tools to also track these changes is currently being explored together with the segregation of database administration and personal access privileges.
5. The Department has obtained quotes and is currently developing a business case for a Disaster Recovery solution for WARS.
6. Significant work has been undertaken to improve the Department's vulnerability management capabilities and database security controls have been incorporated into the ICT Governance Framework to ensure ongoing review and enhancement.

# Auditor General's 2020-21 reports

| Number | Title | Date tabled |
|---|---|---|
| 8 | Regulating Minor Pollutants | 26 November 2020 |
| 7 | Audit Results Report – Annual 2019-20 Financial Audits of State Government Entities | 11 November 2020 |
| 6 | Transparency Report: Major Projects | 29 October 2020 |
| 5 | Transparency Report: Current Status of WA Health's COVID-19 Response Preparedness | 24 September 2020 |
| 4 | Managing the Impact of Plant and Animal Pests: Follow-up | 31 August 2020 |
| 3 | Waste Management – Service Delivery | 20 August 2020 |
| 2 | Opinion on Ministerial Notification – Agriculture Digital Connectivity Report | 30 July 2020 |
| 1 | Working with Children Checks – Managing Compliance | 15 July 2020 |

**Office of the Auditor General**
**Western Australia**

7th Floor Albert Facey House
469 Wellington Street, Perth

Perth BC, PO Box 8489
PERTH WA 6849

T: 08 6557 7500
F: 08 6557 7600
E: info@audit.wa.gov.au
W: www.audit.wa.gov.au

@OAG_WA

Office of the Auditor General for
Western Australia