



Media contact: Natasha Farrell

Mobile: 0427 953 993

Email: natasha.farrell@audit.wa.gov.au

26 November 2020

Audit of the Western Australian Registry System finds significant vulnerabilities

The Auditor General's [Western Australian Registry System – Application Controls Audit](#) report has tabled in Parliament today.

The audit assessed if the Department of Justice had key controls in place over its system housing births, deaths, marriage and change of name information.

Auditor General Ms Caroline Spencer said the audit findings in 2019 were so concerning they were not tabled as part of the office's annual information systems report in May 2019 as planned.

'I considered that publishing the significant findings at that time, when the most serious system vulnerabilities still existed, could expose the system and its dataset to deliberate harm.

'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 West Australians.

'While finding system weaknesses is all too common in our audit work, and I am pleased the Department has now taken action to address many of these vulnerabilities, it was deeply concerning to find such serious shortcomings in a system that houses such sensitive information,' Ms Spencer said.

Some of the original weaknesses identified were:

- inadequate system access controls – with 11 third party vendor staff having full access to the database
- inadequate logging and audit trails to check access or verify that changes to information, such as names and life events, were appropriate and authorised
- no data encryption to protect confidential information

The report includes recommendations for the Department to continue improving various aspects of the system, as well as to develop a disaster recovery plan and review and enhance its vulnerability management process.

It is important to recognise that outsourcing system development and maintenance to third parties does not absolve any public sector entity of the responsibility for strong data governance. All entities must retain in-house risk awareness and capability for monitoring and oversight.

Report resources

- [PDF version](#)
- [summary video](#)