Western Australian
Auditor General's Report

Information Systems Audit Report

Report 23: November 2015

Office of the Auditor General
Western Australia

7th Floor Albert Facey House
469 Wellington Street, Perth

Mail to:
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

National Relay Service TTY: 13 36 77
(to assist people with hearing and voice impairment)

On request, we can deliver this report in an alternative format for those with visual impairment.

ISSN 2200-1913 (Print)
ISSN 2200-1921 (Online)

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Information Systems Audit Report

Report 23
November 2015

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

INFORMATION SYSTEMS AUDIT REPORT

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 agencies to determine if these effectively support the confidentiality, integrity and availability of information they hold.

The first part of this report shows how seven agencies are managing the security of their databases, which contain confidential information about organisations and individual members of the public. We found weaknesses at all the agencies, potentially compromising the security of the information they hold.

Importantly, we have included with this report, specific guidance to agencies on database security which will make it easier for agencies to review their practices and make improvements.

The second part of this report looks at key business applications at four agencies. While we found all four applications were performing well and addressing business needs, we did identify some weaknesses that increase the risk to the confidentiality, integrity and availability of sensitive information.

I trust the content of this report will assist all agencies, and not just those audited, to assess and address any risks with their own IT systems.

I wish to acknowledge the cooperation of the staff at the agencies included in our audits.

COLIN MURPHY
AUDITOR GENERAL
5 November 2015

Contents

Auditor General's Overview

Information Systems Audit reports are an important product of my Office because they identify a range of issues that can seriously affect the operations of government if not addressed.

Unfortunately, we too often see the same or similar types of basic control weaknesses reported each year. Therefore, we have this year prepared some guidance on database security that I encourage all agencies to consider. The guidance is included as an Appendix to this report and will be available as a stand-alone document on our website.

This report contains two items:

- Database Security
- Application Reviews.

The first item of the report shows how seven agencies are managing the security of their databases. Western Australian government agencies collect and store a significant amount of sensitive and confidential information about organisations and individual members of the public. We audited the security of 13 databases that were critical to agency functions and hold personal and sensitive information. They included human resource, finance and operational systems.

We conducted technical analysis of the databases, with the assessment broken into seven key categories. None of the sampled agencies adequately prevented unauthorised access to and data loss from their databases. All agencies had weaknesses across the seven categories. Most concerning was that we continue to find weak controls in some basic, easy to fix areas such as passwords, patching and setting of user privileges.

The second item of the report contains the results of our audit of key business applications at four agencies. We found that all four applications were performing well and addressing business needs.

However, we found some weaknesses around data validation and manual process supporting these applications. As well, issues pertaining to information security were found at every agency. Particular areas of concern were around data access and logging, software patching and updates, and general security practices in agency IT environments.

These weaknesses increase the risk to the confidentiality, integrity and availability of sensitive information that is entrusted to agencies.

All the agencies we audit understand the criticality of their IT systems to their operations and yet, too many underestimate the risks that exist to those systems. I trust that the guidance provided in the appendix to this report will make it easier for agencies to review their practices and improve the security of information they hold.

Database Security

Introduction

Western Australian government agencies collect and store a significant amount of sensitive and confidential information on organisations and individual members of the public. They also perform a variety of financial transactions through computer systems. These agencies have an obligation to secure systems and information from unauthorised access and to prevent it from being inappropriately exploited.

Databases used by agencies to store information are highly desirable targets for cyber-attacks as they offer hackers immediate and significant benefits, such as financial details of organisations and individuals. As we have previously reported, implementing appropriate controls will reduce the risk of unauthorised access and the loss and exploitation of information managed by agencies.

Background

This year, as part of our annual general computer control audits and application reviews, we undertook health checks on 13 databases that store critical information at a sample of seven agencies. Database health checks assess a number of areas to identify weaknesses of most concern. These weaknesses are relatively easy to identify and address.

The objective of this audit was to determine if obvious security weaknesses existed that would allow unauthorised access to the information held in selected databases.

Specifically, we examined the seven key areas set out below:

Attack surface	The greater the exposure the more likely an attempt will be made to break into a system. By reducing the opportunities available to an attacker a database server's exposure is reduced.
Account security	Strong account security is one of the most important aspects of a secure database. This is the first port of call for an attacker to try to gain access to a system.
System hardening	Locking down privileges and ensuring secure configurations are in place make systems resilient to attackers.
Version/patching	Installing vendor security updates are important to prevent attackers exploiting known security vulnerabilities.
Data protection	Databases that store sensitive information can be further protected using a number of methods such as encryption, virtual private databases or data redaction.
Auditing/monitoring	Helps ensure that the information has not been compromised or accidentally exposed. This also helps identify activities in a database and attempted or failed attempts to access the database.
Backdoors/misconfiguration	Attackers will often leave backdoors behind to regain access later. These can look like misconfigurations but need to be checked.

We audited 13 systems at seven agencies, which included nine Oracle and four MS SQL databases. The seven agencies were:

- Murdoch University
- Legal Aid
- Department of Health
- Curtin University
- Department of Local Government and Communities (DLGC)
- Drug and Alcohol Office – now incorporated into the Mental Health Commission
- Department of the Attorney General (DotAG).

The databases we reviewed are critical to agency functions and included human resource, finance and operational systems that hold personal and sensitive information. We analysed various settings on database servers and interviewed staff and contractors regarding their security practices and controls in place.

We provided agencies with detailed reports and recommendations of our findings so they could address them and where required, conduct further investigation. The findings of this audit provide an insight to good practice and the types of control weaknesses and exposures that can exist so that all agencies, including those not audited, can consider their own performance and improve their database security.

We calculated the severity of agency weaknesses using a risk matrix that considered consequences of the risk with the likelihood of it occurring. Weaknesses were rated according to a four point scale; low, medium, high, and extreme. A weakness rated as low is not likely to occur and the consequences will be insignificant or minor. Extreme weaknesses are likely or expected to occur and will have a catastrophic impact on the agency.

This was a narrow scope performance audit, conducted under section 18 of the *Auditor General Act 2006* and in accordance with Australian Auditing and Assurance Standards. Narrow scope performance audits have a tight focus and generally target agency compliance with legislation, public sector policies and accepted good practice.

Audit conclusion

The seven sampled agencies have not adequately protected information from attackers to prevent unauthorised access and data loss. Sensitive and confidential information is at risk and agencies may not know if or the extent to which data is compromised.

We identified 115 findings with failures in all seven key areas. Most concerning was a lack of some basic controls over passwords, patching and setting of user privileges. Our findings also revealed copies of sensitive information across systems and poorly configured databases. We rated these types of weaknesses as extreme or high given how easily an attacker can exploit them to gain the level of access needed to view or modify data.

Key findings

We have structured our findings in line with the seven key areas we tested.

The first four areas; attack surface, account security, system hardening and version/patching represent the greatest risk to databases and the information they contain. It is concerning then, that these four areas make up 64 per cent (73) of the total findings, with 47 per cent (54 of the total 115 findings) rated extreme or high.

Findings by Domain/Severity	Total (%)	Extreme	High	Medium	Low
Attack surface	25 (22)	1	17	3	4
Account security	22 (19)	4	8	–	10
System hardening	17 (15)	6	9	2	–
Version/patching	9 (8)	4	5	–	–
Data protection	13 (11)	–	4	9	–
Auditing/monitoring	27 (23)	–	–	1	26
Backdoors/misconfiguration	2 (2)	–	2	–	–
Totals	**115 (100)**	**15**	**45**	**15**	**40**

Table 1: Findings by severity

Distribution of findings; Extreme=15 (13%) High=45 (39%) Medium=15 (13%) Low=40 (35%)

Each agency had at least three findings that we rated as extreme or high. Figure 1 shows the number and severity of the findings per agency database.

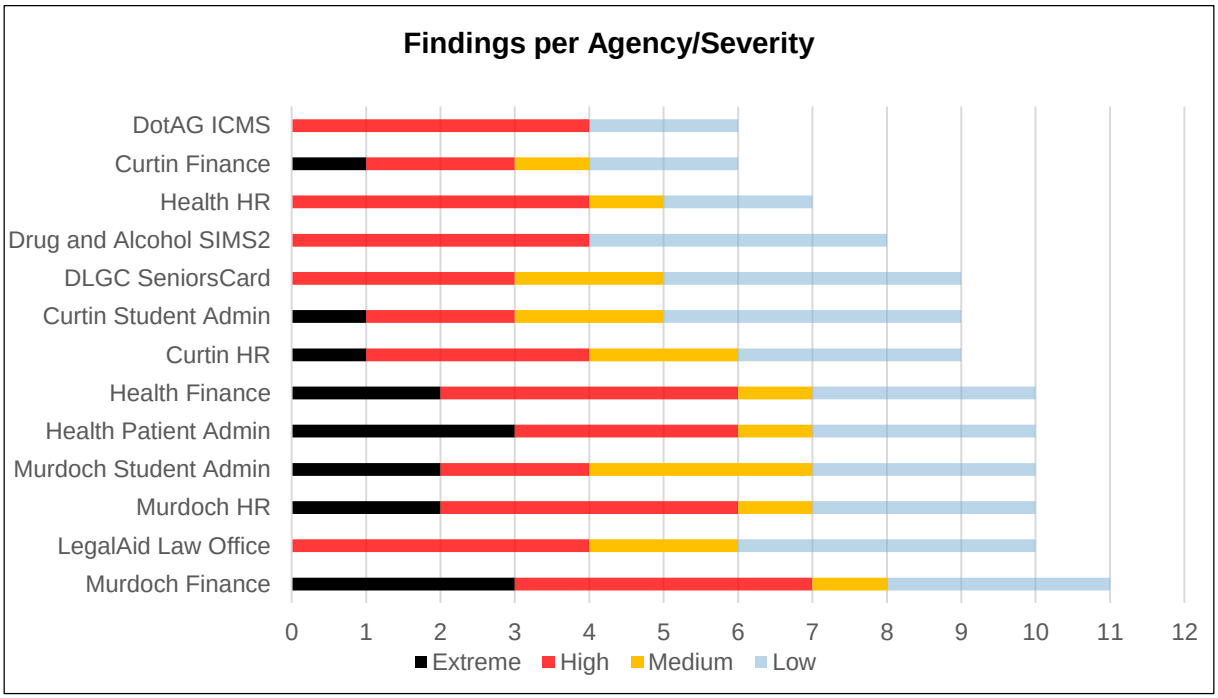

Figure 1: Finding per severity

Attack surface

The greater the attack surface of a system the more likely it is to be compromised. This part of the health check gauges the attack surface by checking what applications and services are installed and accessible.

We found that agencies have increased the risk of unauthorised access and loss of information by increasing the number of opportunities for exploitation. This type of weakness made up 25 (22 per cent) of the total findings of which 18 were rated as extreme or high risk.

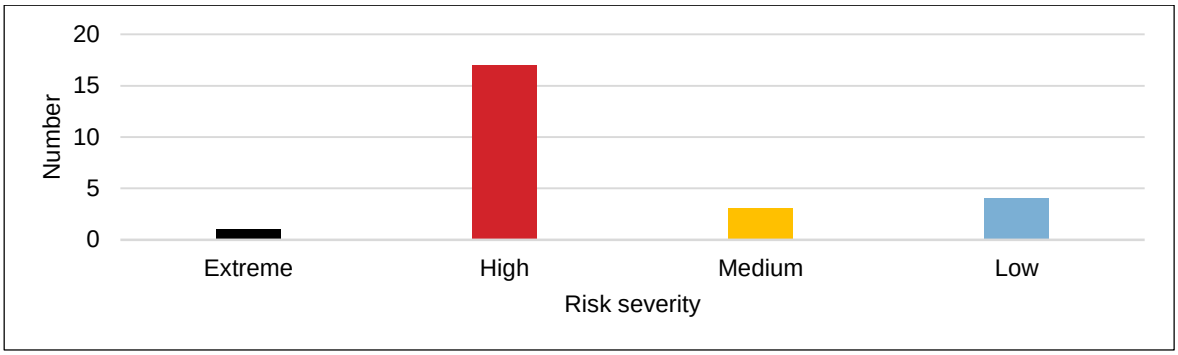

Figure 2: Attack surface findings by severity

We found several agencies did not separate their production, test and development environments. These environments replicated information from production (live) databases across all environments. This increases the attack surface by making the data more freely available to a wider pool of staff and contractors without the same level of security afforded to the production database.

Settings in the database that are disabled by default when installed were enabled without reason. For example, we found settings enabled to allow the execution of operating system commands that permit the extraction of information from the database or to run unsolicited programs. These functions can allow an attacker or a well-crafted piece of malware to perform unauthorised activity leading to the compromise of the server and the data it contains. Alternatively they may be able to use the compromised server as a stage to perform other unauthorised activity across the entire network.

The 'PUBLIC' role in a database gives all users its assigned privileges. We found many databases that have allocated Read/Write privileges to PUBLIC, thereby providing all users with highly privileged access and creating information security risks. We also found instances where this account was allocated access to network folders, which creates additional vulnerabilities and introduces data integrity risks.

We found database links accessible by PUBLIC in a small number of databases. This allows access from one database to other connected databases so anyone with access to one may access the other. This includes the execution of programs to compromise information held in the databases within the local network or from other external networks and the Internet.

Databases contained unused schemas and automatic procedures, which can lead to a full compromise of the server. Schemas are the 'blue print' for how information is structured in a database, thereby increasing the exposure of information to attackers. These types of weaknesses also increase the likelihood of security vulnerabilities in the databases further increasing the risk of information being exploited.

We found a number of database servers that have multiple unrelated application databases. This increases the connections and activity on the database server and the likelihood of unauthorised access or cyber threats in general. It is better practice for each production database, if critical to the operations of the agency, to have its own dedicated server when the information it contains is sensitive.

There were no firewalls segregating databases and servers from the rest of the network or other agency networks. Users that access the network can compromise services running on the database or the server itself. This increases the risk of someone attempting to gain unauthorised access to the database or its server due to the increased number of people that have access to the server or use the same network.

Account security

Account security examines if database user accounts have default or easy to guess passwords. Exploiting weak passwords are one of the first actions an attacker will try in order to gain system access. Strong account security is therefore one of the most important steps to take to secure a database server.

The security of database users and system accounts could be improved across all systems we audited. We found a large number of accounts with high level privileges to data and system settings that had weak password controls. Account security made up 22 (19 per cent) of the findings of which 12 were rated as extreme or high risk and 10 as low.

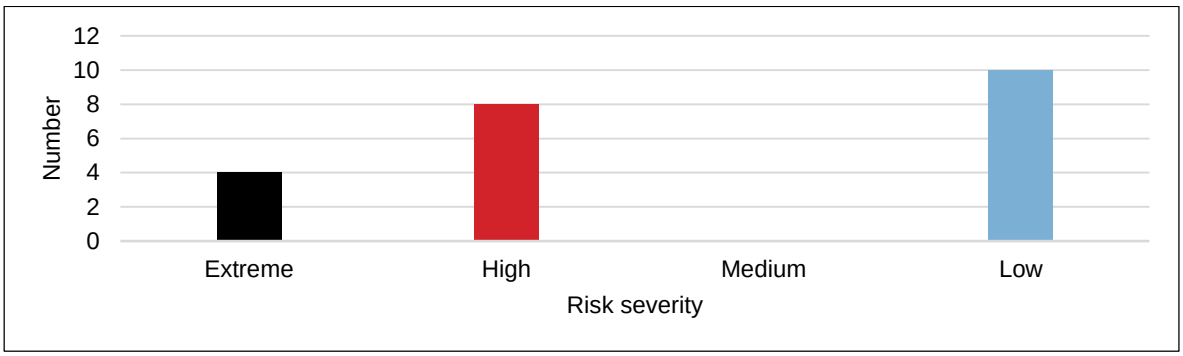

Figure 3: Account security findings by severity

We found many instances of database administrator accounts where the default usernames and passwords were still in use. These default user settings are widely known and often the first accounts someone would try to exploit. We also identified accounts with exceptionally easy to guess passwords. Examples include passwords that were the same as the username, passwords that were the same name as the application and passwords such as ‘test’, ‘password1’, ‘sqladmin’.

There were also many three-character passwords; in particular, one Database Administrator Account (DBA) had a password of ‘DBA’. There were several instances where the ‘SYS’ password was too easy to guess. The ‘SYS’ account carries DBA privileges and cannot be locked out. This provides an attacker with unlimited attempts to brute force the password. We also found instances where weak passwords had never changed or had been the same for 6-12 years. The risk of a password being compromised through brute force attacks, disclosed by trusted users or extracted from hacked systems increases with its age. Periodic password changes mitigate these risks.

We examined various properties in databases and found that password aging had not been enforced across many of them. We found several agencies had not changed administrator account passwords anywhere from three to over 10 years. In one database, we found 17 highly privileged accounts that had never had their passwords changed.

We also identified a large number of inactive user accounts, which had weak passwords or not had their passwords changed. While many accounts we identified on Oracle Databases were ‘locked’, flaws in the configuration of the database may allow attackers to unlock them. An attacker that has access to an existing account can exploit these flaws to unlock other accounts. These additional accounts might have higher levels of access than the attacker’s account, or allow the attacker to go undetected by occupying an unused account.

Several agencies were not logging accounts to determine activity within their database, meaning that they were not aware of when and what is accessed and if there was unauthorised activity occurring. Further detail is included under the Auditing and Monitoring section of this report.

What can happen when security is inadequate – a case study

At one of the agencies, we guessed passwords assigned to a number of accounts and were able to gain access to the network. The password of two of the accounts was ‘password’ which we guessed on the first attempt. After compromising the first account, we notified the agency and advised them to eliminate the use of this password.

We used the second of the compromised accounts to logon and browse information stored on the network. Within a short time we found thousands of highly confidential and sensitive records about individuals including minors which should only be accessible to a small number of authorised staff.

We also found database scripts and system configuration files which could help to compromise sensitive databases and systems. We then connected a USB device to copy thousands of records off the network without detection. We performed the same process a week later to see if the agency had identified and taken any appropriate action against this kind of data loss – it had not and we were able to perform the same operation again.

Figure 4: Sensitive information lost after password easily guessed

System hardening

Locking down privileges and ensuring secure configurations are in place make systems more resilient to attackers and cyber threats.

We found default configurations and permissions at 10 out of 13 systems audited indicating that the databases were not properly hardened. Inadequate system hardening made up 17 (15 per cent) of the findings of which 15 were rated as extreme or high risk and two as medium.

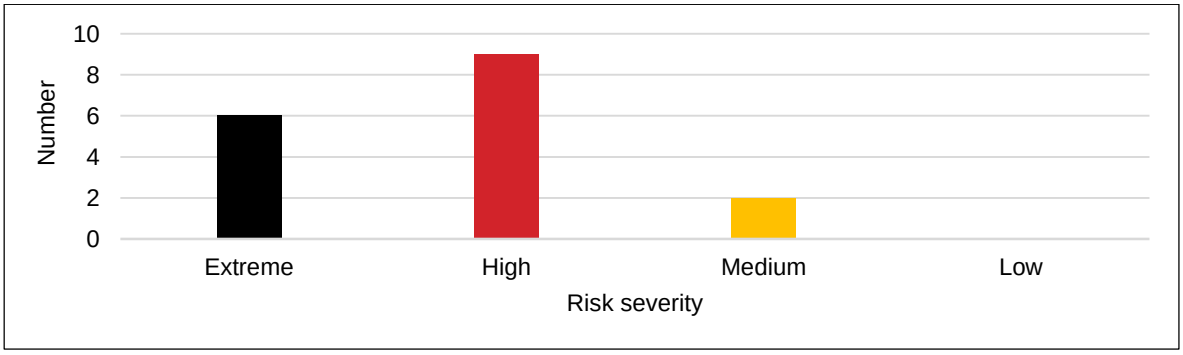

Figure 5: System hardening findings by severity

Excessive privileges were granted to the PUBLIC role across most systems. This could allow an attacker to compromise the entire database. On these systems it is possible to execute procedures to allow anyone to grant themselves arbitrary java privileges with the ability to load and execute programs. This can lead to a full compromise of a database server.

We found several examples where the PUBLIC role had privileges on various database tables owned by highly privileged accounts such as ‘SYSTEM’ and ‘SYS’. If PUBLIC has high privileges on a table, it means that queries can be run to extract information from those database tables and even allow the creation of unauthorised accounts and permissions.

Database administrator accounts

Databases generally come with pre-configured administrator accounts and passwords that are listed in product documentation and widely available on the Internet. Because attackers will normally try the default user names and passwords, it is important to change these on installation.

In discussions with database administrators at the seven agencies, we found it common for their accounts to be used for general user activity and not solely for administrative tasks. This means that agencies cannot attribute actions to specific individuals or hold them accountable.

It is important to use database administrator accounts exclusively for administrative tasks with standard database accounts. Ensuring database administrators have unique and identifiable accounts will assist in auditing activities of databases. This is particularly helpful during investigations relating to an attempted, or successful intrusion. Furthermore, database administrator accounts should not be shared across different databases as this can increase the likelihood of a successful attack on multiple databases.

Version/patching

Attackers take advantage of security vulnerabilities to gain access to systems and escalate their privileges. As new vulnerabilities are discovered, it is important to keep software up to date by upgrading outdated software to the latest versions and regularly installing vendor supplied security patches.

Only four of the 13 systems reviewed were completely patched. The other nine were missing vendor patches, some dating back to 2010. Patching made up nine (8 per cent) of our findings with all of them rated either extreme or high risk.

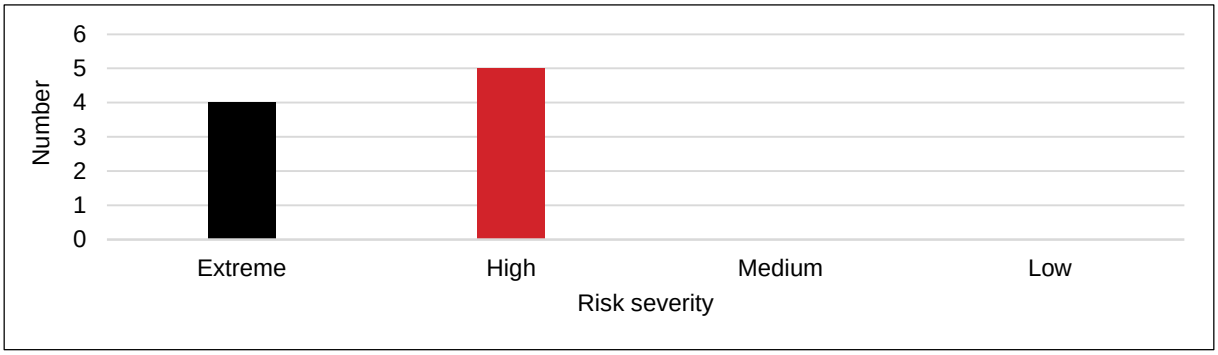

Figure 6: Version/patching findings by severity

We found one database that was never patched. This server was susceptible to numerous critical security vulnerabilities that an attacker with just a low access privilege could exploit to gain full control over the server.

We found several systems running a version of Oracle that ceased mainstream support in 2012. There are numerous known vulnerabilities in this version including many critical security flaws.

In one agency, all of its 150 databases stored large amounts of sensitive information without mainstream support from their respective vendor. Over half of these systems were so old the vendor gave no support at all. This significantly increases the risks to information stored in these databases.

We found two SQL servers that were over two years behind on patches and one three years behind. All three servers should have received numerous patches.

Many of the security vulnerabilities in the nine systems that were not fully patched have been well known in the industry since 2010. The Australian Signals Directorate (ASD) has identified patching of systems as one of the top four measures agencies can take to protect their information.

> Leaving applications unpatched will dramatically increase the attack surface of the system and any interconnected system. Malicious intruders often take advantage of vulnerabilities in applications to gain a foothold on a network, from which they can attack other systems within the organisation's network.[1]

Figure 7: The Australian Signals Directorate on why patching is important

Data protection

Sensitive, confidential or secret data requires a secure database server. Databases can be further protected with the use of encryption, virtual private database and or data redaction.

None of the 13 systems were encrypting sensitive data stored within their databases or on backups stored on tapes and off site. We also found inadequate protection of production data found in development and test environments.

Data protection findings made up 13 of the 115 findings (11 per cent) with four rated as high and nine as medium.

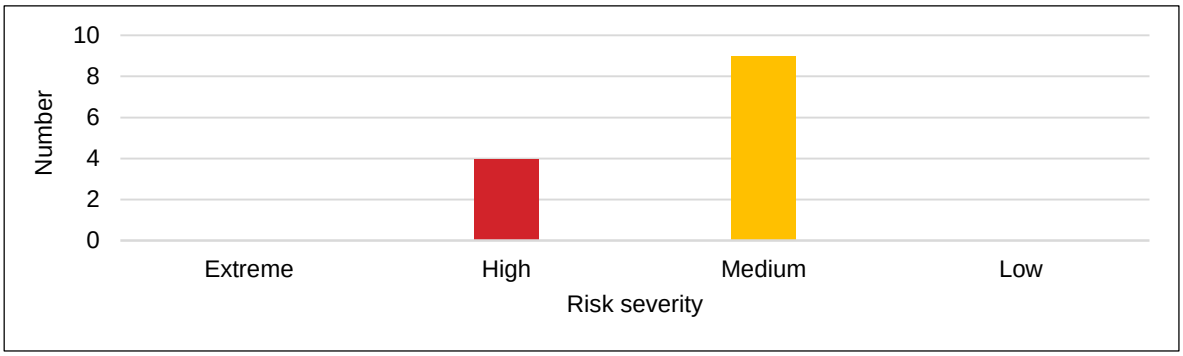

Figure 8: Data protection findings by severity

Auditing and monitoring

Database auditing enables an administrator or security manager to detect in a timely manner the possible security breach of a database and to audit access made to the data. It means that the administrator can answer questions like, 'has data been accessed by an unauthorised person, has data been changed, who changed it and when'.

Database object auditing was not active on any of the 13 databases we reviewed. While some actions such as failed logins were recorded in some cases, auditing was not active on sensitive data stored within the databases.

Auditing and monitoring weaknesses made up 27 (23 per cent) of our findings of which 26 were rated as low risk. However, these risk should not be underestimated because without adequate security monitoring, agencies will not know if, or to what extent, their information is compromised.

[1] Australian Signals Directorate: Top 4 Strategies to Mitigate Targeted Cyber Intrusions: Mandatory Requirement Explained, July 2013

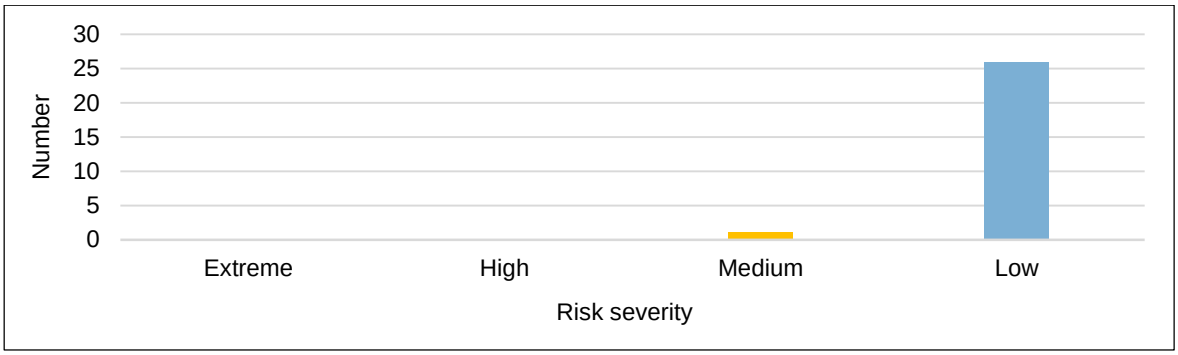

Figure 9: Auditing and monitoring findings by severity

Backdoors/misconfiguration

Once an attacker has broken into a database, they may leave a backdoor in the system to allow access at a later date. These backdoors can take many forms and often look like misconfigurations. This section reviewed aspects that may be a backdoor but if not are more than likely an undesirable misconfiguration.

There are a number of ways to 'backdoor' a database server. Occasionally a misconfiguration can look like a backdoor and usually is the result of a mistake.

We only found instances at two agencies where misconfigurations existed. These had the PUBLIC role assigned membership to 'other' roles. Any privileges granted to these 'other' roles are therefore effectively granted to everyone on the database server via the PUBLIC role.

Both instances were not default settings of a database and therefore were deliberate actions. The reasons and real impact of these misconfigurations are not known so are considered to be high risk. We recommended to both agencies that they investigate these instances and correct as appropriate.

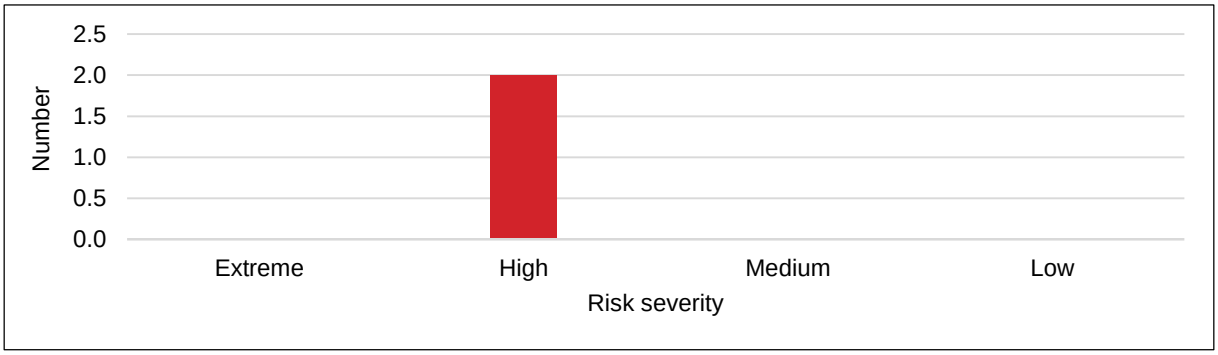

Figure 10: Backdoors/misconfiguration findings by severity

Recommendations

1. **Agencies need to understand the risk profile of information they manage and ensure appropriate controls are in place to protect this information. Based on the risk profile of the information, agencies should determine and implement adequate controls over databases and systems to prevent serious exposures that could lead to the compromise of information managed by agencies.**

2. **Specifically, agencies should:**

   a) **use the principle of least privilege and grant only those privileges needed to perform the business requirements of a role. All user accounts (active/locked) should be given strong passwords and set to expire**

   b) **assess, test and deploy vendor security updates in a timely manner to prevent attackers exploiting known security vulnerabilities**

   c) **assess risks with configuration options on the database and determine if it is actually required to be enabled. Locking down privileges and ensuring secure configurations are in place make systems resilient to attackers**

   d) **not use information in production databases in testing or development databases unless the testing or development environments are accredited to the same standard as the production environment**

   e) **place database servers behind network or application level firewalls and only provide access to systems and users that have business requirements to do so**

   f) **further protect databases that store sensitive information using a number of methods such as encryption, virtual private database or data redaction. If live data is to be used for development purposes, it should be disguised so that it cannot be used inappropriately.**

Agency responses

Curtin University

Curtin acknowledges fully the requirement to ensure the security of its sensitive information stored in its financial, human resources, and student management systems in accordance with the University's extant risk, legislative, and regulatory environments. To this end, we are taking proactive steps to address the OAG's findings related to Database Security in a pragmatic, risk-informed, and operationally-sensitive manner.

Department of the Attorney General

The Department of the Attorney General has valued the opportunity for external review of its performance. It is pleasing to note that the Auditor General has found that the ICMS database security controls, in several areas of focus, were found to be effective.

The Department has already implemented many months ago several of the recommendations made by the Auditor General and a departmental risk assessment will be undertaken to determine whether any further risk mitigation strategies are required.

Department of Health

The Department of Health welcomes the opportunity to work with the OAG to review internal controls around information contained in WA Health databases

The Department accepts the recommendations and notes the overall rating of moderate with respect to database security contained within the 2014/15 Information Systems Audit.

The Department proposes establishing a working group to address the recommendations. Whilst some of the recommendations can be addressed and implemented in the short term, others may require additional resources to be acquired. These more complex implementations will be considered within WA Health's ICT reforms, as outlined in the 2015-18 ICT Strategy. The recommendations will be assessed within defined affordability parameters against other ICT priorities that are focused on stabilising existing systems and infrastructure.

Department of Local Government and Communities

The Department of Local Government and Communities accepts the Auditor General's Summary of Findings in relation to database security.

At the time of the performance audit, the department was not administering the databases. Upon assuming responsibility for the databases, the department has addressed the findings identified during the performance audit, specifically:

- User access is restricted to a needs basis, reviewed on a regular basis, and complies with contemporary account management practices. Generic or group access accounts are not permitted.
- Security and software updates are tested and applied as soon as practicable.
- All database configuration settings are deliberately assessed and configured to ensure appropriate security.
- The same security protocols are maintained across test and production environments. Test systems are deleted when no longer required.
- All data servers are maintained behind appropriate firewalls.

- All database backups are encrypted.
- The department is contracting for vulnerability and penetration assessments to test and improve its database security.

The Department of Local Government and Communities is committed to protecting the privacy its data and the security of its databases.

Legal Aid Commission

The Legal Aid Commission accepts the findings of the audit and would like to express its thanks to the Office of the Auditor General for its efforts and advice. Legal Aid is acting on the recommendations and conducting an ongoing review of database security to ensure that sensitive and confidential client information is adequately protected.

Mental Health Commissioner

The Mental Health Commission acknowledges the findings of the performance audit, relating to SIMS2 database security, and accepts all of the review's recommendations. The audit process has highlighted a number of issues and activities are ongoing to resolve those highlighted in the review.

Earlier this year, a project was initiated to upgrade the infrastructure and database management system upon which SIMS2 has been developed. The installation and testing of these new technologies is underway with implementation due to be completed in early 2016.

A number of other items identified in the audit have already been addressed and the remainder will be finalised, as per the review's recommendations, by June 2016.

Murdoch University

Murdoch engaged the services of an independent technical consultant to review the OAG findings and recommendations. A report from this review was produced early this year detailing the technical actions to be taken. Some of the actions have been completed, including the acquisition of a comprehensive password management system.

Many of the remaining actions require specialist technical skills which are being sought. Some of the OAG recommendations required referral to the individual system vendors as the recommendations involved changes to their proprietary software. Murdoch have received the vendor responses and have considered these responses as part of the remediation actions.

Application Reviews

- **Integrated Court Management System** – Department of the Attorney General
- **LAW Office** – Legal Aid Commission Western Australia
- **WA Seniors Card Management System** – Department of Local Government and Communities
- **Services Information Management System 2** – Drug and Alcohol Office of WA

Introduction

Applications are the software programs that facilitate an organisation's key business processes. Typical administrative processes that are dependent on software applications include finance, human resource, licensing and billing. But applications also facilitate specialist functions that are peculiar and essential to individual entities.

Each year we review a selection of key applications that agencies rely on to deliver services to the general public. Our focus is on the application controls designed to ensure the complete and accurate processing of data from input to output. Failings or weaknesses in these controls have the potential to directly impact other organisations and members of the general public. Impacts range from delays in service to possible fraudulent activity and financial loss. This report describes the results of key application reviews at four agencies.

What did we do?

We reviewed key business applications at four agencies. Each application was selected on the basis of the sensitive information that it contains and the impact on the agency or the public if the application was not managed appropriately.

Our application reviews look at the step by step processing and handling of data to ensure that:

- **Policies and Procedures** – Appropriate policies and procedures are in place to support reliable processing of information.
- **Data Preparation** – Controls over the preparation, collection and processing of source documents are accurate, complete and timely before the data reaches the application.
- **Data Input** – Data entered into the application is accurate, complete and authorised.
- **Data Processing** – Is processed as intended in an acceptable time period.
- **Data Output** – Output including online or hardcopy reports are accurate and complete.
- **Interface Controls** – Controls are suitable to enforce completeness, accuracy, validity and timeliness of data transferred.
- **Master File Maintenance** – Controls over Master file integrity are effective which ensure changes are approved, accurate and complete.
- **Audit Trail** – Controls over transaction logs ensure transaction history is accurate and complete.
- **Segregation of Duties** – No staff performed or were capable of performing incompatible duties.
- **Backup and Recovery** – The system/application can be recovered in the event of a disaster.

The four agency applications we reviewed were:

1. **Integrated Court Management System** – Department of the Attorney General
2. **LAW Office –** Legal Aid Commission Western Australia
3. **WA Seniors Card Management System –** Department of Local Government and Communities
4. **Services Information Management System 2 –** Drug and Alcohol Office of WA.

Figure 11 shows the focus of our application reviews: people; process; technology and data. In considering these elements, we follow the data from input, processing and storage to outputs. We also looked at whether sensitive information was properly secured during each step of the process.

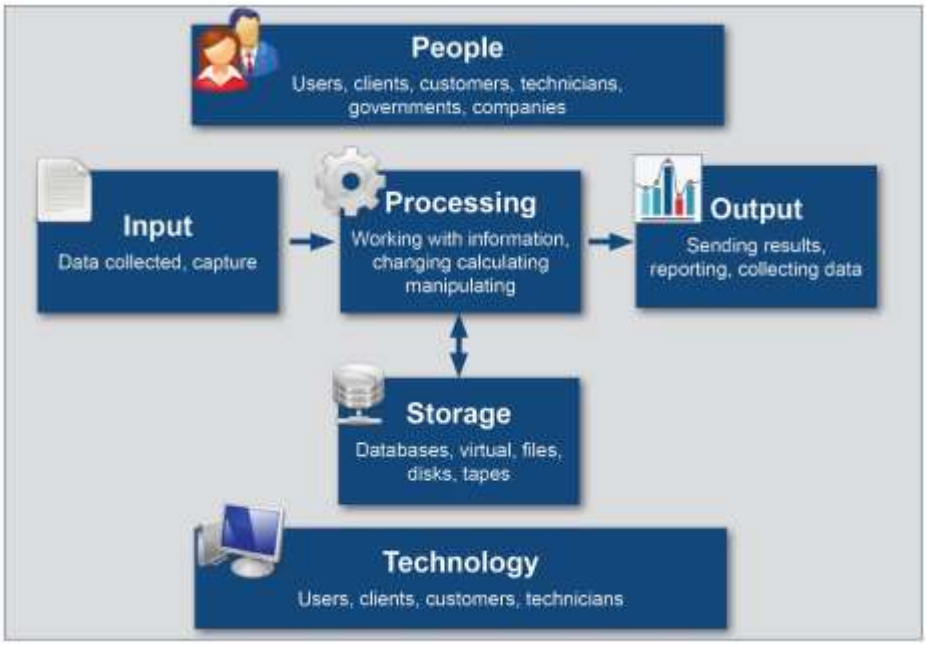

Figure 11: Key elements of focus for our application reviews

Overall assessment

All four applications had some control weaknesses with the most common being poor access controls and monitoring of activity. These weaknesses compromised the security of sensitive information. We also found issues with operational, procedural and process controls that aim to ensure the applications function effectively. Correcting most of the issues we raised is relatively simple and inexpensive. Table 2 summarises our findings against each of the applications.

Area of Focus	ICMS	LAW Office	SIMS	Seniors Card
Policies and Procedures				
Data Preparation				
Data Input				
Data Processing				
Data Output				
Interface Controls				
Master File Maintenance				
Audit Trail				
Segregation of Duties				
Backup and Recovery				
Security of sensitive information				

Table 2: Summary of findings for each business application

Key: No Issues found Issues found

Integrated Court Management System – Department of the Attorney General

Background

The Department of the Attorney General's (DotAG) role is to provide justice, legal, registry, guardianship and trustee services to meet the needs of the community and the Western Australian Government. Its responsibilities include management of the Integrated Court Management System (ICMS) which is used in all criminal and civil jurisdictions for the Supreme, Children's and Magistrates Courts and the states Administrative Tribunal in Western Australia. ICMS supports the management of court cases, tribunals and debtors payments and integrates with systems across the entire Justice network.

ICMS holds personal and sensitive information regarding WA Court proceedings and outcomes. External agencies such as Western Australia Police, the Department of Corrective Services, the Office of the Director of Public Prosecutions and several other parties also access and use the system. This broader access requires appropriate layers of security in ICMS and its related systems to protect sensitive information. Building security into various layers of access to and within a system is known as 'defence in depth'.

The idea behind the defence in depth approach is to defend a system against any particular attack using several independent methods. Defence in depth measures should help prevent security breaches, and also assist an agency to detect and respond to an attack, thereby reducing and mitigating the consequences of a breach.

Audit conclusion

Overall, ICMS is an effective application for managing Court matters and processes. However, DotAG does not follow the good practice principle of defence in depth to protect the ICMS system and information. As a result, we noted a number of control weaknesses in key layers of security across the organisation. While the Department had also identified a few of these risks, most were not previously known. Combined, these increase the risk of unauthorised access and disclosure of sensitive or personal data, such as fines issued to individuals, and their name, drivers licence number, date of birth and address details. They may also impact the integrity and availability of ICMS information.

Key findings

Sensitive information at risk

Our security assessment of the three main ICMS databases, system servers and supporting components identified a range of vulnerabilities and weaknesses across the system. These issues significantly increase the risk to the confidentiality, integrity and availability of sensitive information. This sensitive information includes personal details of individuals involved in ongoing and upcoming court cases.

Some of the weaknesses we noted were:

- **Software updates** – We found that software updates released by the vendor to fix known security vulnerabilities had not been applied and that DotAG were not aware of this weakness. It is far easier for attackers to exploit systems that don't have the latest software patches applied. This may allow attackers to gain unauthorised access to the system and/or information. An effective patching process that keeps software up to date is vital to help protect against cyber and other threats.

- **Weak passwords** – We also found that a number of database level accounts had simple, well-known or easy to guess passwords. If the passwords are obtained or guessed, they can be used to access the system and information. Some of these accounts permitted access to DotAG's data warehouse, as well as access to core ICMS information. The data warehouse stores a wide range of sensitive information from ICMS and various other DotAG systems.

- **Database auditing** – DotAG has not established database level auditing to track direct access and changes to ICMS information. This means it is not possible to identify any inappropriate database level access or modifications to ICMS information. A number of users including external contractors and staff of other agencies have access to the database. This increases the risk and the need for appropriate database level auditing to be implemented.

- **Application level firewall** – ICMS is not protected by an appropriate application level firewall. Given the current control weaknesses and the number of other agencies that can access DotAG's network, deploying an application level firewall would provide an extra layer of security. This would help reduce the risk of unauthorised system access. We also established that information was not being encrypted which means that anyone who accesses this information can read it.

Human resource security procedures

DotAG has inconsistent human resource security procedures. Applying appropriate and standardised human resource procedures helps reduce the insider risk of inappropriate access to and disclosure of sensitive information.

Some of the variances and weaknesses in procedures we identified were:

- **Police clearance requirements** – DotAG policy only requires staff who started after 1 January 2014 to obtain a Police clearance every five years. The employment contract for staff who commenced employment prior to 1 January 2014 does not require them to provide regular police clearances. However, if staff who commenced prior to this date change roles such as through a promotion and this requires a new employment contract, then the new contract will oblige them to obtain a police clearance every five years. Police checks enable employers to assess whether an employee's criminal history is a risk to their operations.

- **Clearance requirements for IT contractors** – DotAG also requires certain staff to obtain a Government Security Vetting which is a higher level of clearance. However, this is not required for the IT system administrators who are DotAG contractors. Inadequate background checks of these individuals poses a significant security risk given that these individuals have full access to DotAG's systems and information.

- **Termination of access** – The Australia New Zealand Policing Advisory Agency recommends[2] that all relevant individuals sign to acknowledge they understand their obligations when they leave an entity's employment. By signing this statement, the individual acknowledges that they may no longer access the entity's systems and may not use any information they became aware of during their employment or engagement for other purposes. DotAG does not require exiting staff or contractors to sign this sort of statement.

[2] Making your company technology crime resistant, 2014.

Controls to ensure ongoing operations

DotAG has not developed an IT disaster recovery plan (DRP), despite ICMS being an important application for DotAG and a number of other organisations. A DRP is a key document that provides details of the procedures to be followed to recover the system in the event of an incident or disruption. With the weaknesses we identified, there is a greater risk of an unplanned event that could affect the availability of the system and impact DotAG's business operations and the other organisations that use it.

Other findings

In addition to the findings we made during the audit, we noted that the Department had also identified some risks associated with the ICMS:

- DotAG had not implemented controls to ensure that confirmations of criminal outcomes were entered into ICMS within one business day of the respective Court hearing. Up to date information on criminal outcomes is critical to WA Police, Department of Corrective Services, Public Prosecution and DotAG's Fines Enforcement Registry. ICMS also does not have automated notifications for transaction processing errors. This may impact the integrity of information within dependant systems.
- The ICMS Portal provides DotAG and external parties such as WA Police with the ability to view ICMS records via the Internet. The process to remove access to the ICMS Portal for external users is not within DotAG's full control and relies on the external agency's processes. This may result in external user accounts remaining active and allow unauthorised access to ICMS information.
- The ICMS system administrator provides role-based user access for ICMS based on their interpretation of an access request. This is because DotAG has not documented what access a user requires to perform their functions. In addition, there is no process to review user access levels periodically to ensure they are appropriate. This increases the risk that users have excessive or inappropriate ICMS access.

DotAG advised that it has addressed these other findings since the audit.

Recommendations

1. **To reduce the risk of unauthorised access and loss or changes to information, the Department of the Attorney General should by the end of 2015:**
   a) **undertake a security risk assessment and use this to apply a defence-in-depth strategy which considers application level firewalls and encryption of data**
   b) **conduct regular vulnerability scanning as defined in its internal policy and implement an appropriate and effective patching process.**
   c) **apply password management controls to ensure that all account passwords follow good practice for access management and comply with internal policy requirements**
   d) **audit and track direct database access to system information.**
2. **To ensure ongoing operations and reduce the risk of inappropriate insider access, by the end of 2015, DotAG should also:**
   a) **develop a disaster recovery plan for its key applications and services to ensure the timely recovery of systems following an incident or outage**
   b) **consistently screen staff and contractors. Current exit procedures should also be enhanced to ensure that staff and contractors are appropriately informed of their IT and information obligations once their engagement ceases**
3. **DotAG should refer to the Australian Signals Directorate for good practice security guidelines.**

Agency response

The Department of the Attorney General has valued the opportunity for external review of its performance regarding the management of application controls of the Integrated Court Management System. It is pleasing to note that the Auditor General has found that ICMS application controls, in several areas of focus, were found to be effective.

Several of the findings reported by the Auditor General were previously reported by the Departments Internal Audit and were addressed prior to the completion of this audit.

The Department notes the Auditor General's key findings regarding access controls and monitoring of activity and will consider the recommendation to the Department following a risk assessment.

LAW Office – Legal Aid Commission Western Australia

Background

The Legal Aid Commission of Western Australia (Commission) provides legal information, advice, assistance and representation to the public. The type and level of help an individual receives depends on their legal problem, their finances, and the Commission's resources. The Commission aims to make it easier for people to obtain legal help and resolve their problems as soon as possible. It also tries to find alternatives for clients than going to Court.

The legal aid process includes assessing the eligibility of applicants, whether an applicant should co-contribute to the costs of legal representation and assigning lawyers to represent an applicant. The software application used by the Commission to help process requests for legal aid is called LAW Office. An applicant's details are entered into LAW Office to assist with assessing the eligibility of applicants to receive legal aid and assigning a lawyer. It also calculates any co-contribution that may be required. The system was co-developed with other Australian Legal Aid Commissions.

In order to qualify for a grant of legal aid the following eligibility tests are applied to each applicant:

- Whether the legal matter is in one of the priority categories that the Commission has to provide aid for or whether appropriate assistance can be obtained elsewhere.
- A means test to determine if the individual can afford a private lawyer, and whether a co-contribution is required.
- Merit test to establish whether the individual's case is likely to succeed.

In 2013-14, State Government funding for legal aid was $38.150 million and Commonwealth grants and contributions totalled $22.182 million. In this period the Commission received 14 059 applications for legal aid, and approved 71 percent of these requests.

Audit conclusion

Overall, LAW Office is an effective application for managing legal aid applications. However, some control weaknesses in data validation and supporting processes could result in legal aid being incorrectly or unfairly awarded. Due to a lack of oversight there is also a risk that external firms appointed to provide legal advice may not be meeting defined levels of service or quality. In addition, a number of system and database vulnerabilities were identified. These increase the risk of unauthorised access and sensitive client information being compromised.

Key findings

Data validation

The Commission does not have an effective process to validate information and documents provided by individuals applying for legal aid. For example, the Commission accepts an applicant's declaration of assets and only cross-checks this information on an exception basis. Our own data matching of applicant information with land ownership records found that 63 of the 14 059 applicants owned property they did not declare. The Commission advised that often properties are co-owned with a person who is the opposing party in a legal suit, and these should not be used in means tests.

Without appropriate validation, there is a risk the Commission will provide legal aid to people who are not eligible. But as well, because legal aid funding is limited, any allocation of financial assistance to people who should not qualify for assistance means that more deserving people will miss out.

Decisions and calculations based on unchecked information

The Commission does not have an effective process to review the accuracy and completeness of applicant information recorded in the system. Errors in the applicant's information or the transcription of the information into the system can impact on the fairness of internal decisions based on this information.

Assessors use LAW Office information when deciding to approve or decline legal aid representation and in assigning lawyers. The system also uses this information to calculate the amount of any client co-contribution. Inaccurate information entered into the system increases the risk of inconsistent or inappropriate decisions by assessors in awarding legal aid. It is also likely to affect the accuracy of the co-contribution amount.

Compensating review processes

Lawyers are able to access the system and enter applications for aid on behalf of their clients. As a control to check that entered information is accurate and complete, the Commission checks the accuracy of a sample of the information entered by firms that provide legal aid services to clients. The review also checks whether lawyers comply with policies and procedures for providing services to clients, and in claiming compensation for services provided.

However, the sample that is checked is small – just five of the 27 private practitioners that the Commission received complaints against in 2014, down from 10 in the previous year. Although this number is relatively small, the Commission also rolled out new private practitioner panel arrangements that set out specific obligations on panel members.

The small sample means that the Commission can give only minimal assurance about the accuracy of information or the quality of service provided to clients. The small sample also impacts on the assurance the Commission can give that the firms accurately charge for legal services they provide.

Security of sensitive information

We performed a vulnerability assessment and database security check on the LAW Office application and the related IT environment. These tests identified a range of weaknesses which increase the risk to the confidentiality, integrity and availability of sensitive client data.

Some of the weaknesses we noted were:

- **Software updates not applied** – We found that software updates released by the vendor to fix known security issues and weaknesses had not been applied. This may allow attackers to gain unauthorised access to the system and/or information. An effective patching process that keeps software up to date is vital to help protect against cyber and other threats.
- **Weak passwords** – We also found that a number of database accounts had simple, well-known or easy to guess passwords. If the passwords are obtained or guessed by hackers, they can be used to access the system and information.
- **Data is not encrypted** – Despite storing a large amount of sensitive client information the Commission had not applied any encryption to stored data. Encryption would help prevent sensitive client details being read by unauthorised individuals.

Human resource security procedures

We identified that the Commission do not require staff or relevant individuals to sign to confirm they understand their obligations when they leave the entity's employment. By signing this statement, the individual acknowledges that they may no longer access the entity's systems and may not use any information they became aware of during their employment or engagement for other purposes. The Australia New Zealand Policing Advisory Agency recommends[3] that all relevant individuals sign to acknowledge they understand their obligations when they leave.

We also found that an IT account belonging to a former staff member was still active, although the activity logs showed that their last login was on their last day of employment. This account could have been used to gain unauthorised access to the Commission's network and the LAW Office application. Without adequate procedures covering all individuals ending their employment or engagement, there is an increased risk of unauthorised system access. This may impact the confidentiality, integrity and availability of sensitive information.

Recommendations

1. **To reduce the risk of unauthorised access and changes to information, the Legal Aid Commission Western Australia should by September 2015:**

    a) **implement an appropriate and effective patching process. The Commission should also conduct regular vulnerability scanning as defined in its internal policy**

    b) **apply password management controls to ensure that all account passwords follow good practice for access management and comply with internal policy requirements**

    c) **protect sensitive information by considering encryption for data at rest and for backups**

    d) **enhance current exit procedures to ensure staff and contractors are appropriately informed of their IT and information obligations once their engagement ceases. In addition, all IT user access accounts belonging to terminated employees and contractors should be deleted or disabled in a timely manner.**

2. **To ensure completeness and accuracy of LAW Office information, the Commission should by September 2015:**

    a) **implement appropriate checks to validate each applicant's information and supporting documentation. This should be supported by an internal review process to give confidence that decisions regarding legal aid allocations are made fairly and appropriately**

    b) **establish a robust and appropriate review process of law firms that it allocates funds to. This should help ensure that the Commission and their clients are receiving appropriate levels of quality and value in contracted services.**

[3] Making your company technology crime resistant, 2014.

Agency response

The Legal Aid Commission accepts the findings of the audit and would like to express its thanks to the Office of the Auditor General for its efforts and advice. The report highlights the need for ongoing review of systems and processes to ensure that clients receive the most appropriate service and the best possible outcome. Legal Aid will act on the recommendations as a matter of priority to improve the assessment of legal aid applications and reduce the risk of client information being compromised.

WA Seniors Card Management System – Department of Local Government and Communities

Background

The Department of Local Government and Communities (the Department) is responsible for managing the Western Australian Seniors Card system, and ensuring that card holders remain eligible.

In May 2014, the Department purchased a new Customer Relationship Management system. The Department customised this system to manage the Seniors Cards. The system is used to collect and store applicant information. Seniors cards are printed using this information.

Approximately 360 000 seniors hold a Seniors Card in Western Australia. The card provides WA senior citizens with a range of government concessions, rebates and discounts such as free public transport, driver's licenses and car registration discounts, rebates on personal safety devices as well as discounts at over 500 businesses in WA.

The value of Seniors Card concessions and rebates on government services is over $20 million a year, a figure which should rise as the Department expects the number of people qualifying for a card to increase, despite a tightening of the eligibility criteria[4].

During the period of audit, applicants for a Seniors Card were assessed against the following criteria:

- aged 60 years or more
- a permanent resident of Western Australia
- works 25 hours or less per week, averaged over the year.

Card holders are not required to renew the card but they are required to inform the Department if their circumstances change and they become ineligible for the card.

A consequence of the Department's role in administering the Seniors Card is that they are required to hold sensitive information on thousands of WAs senior citizens. Securing this information is an important obligation on the Department.

Audit conclusion

A range of control weaknesses impact on the security of information contained in the Seniors Card system. These weaknesses increases the risk of inappropriate access to and potential misuse of Seniors Card holder's personal information and could expose seniors to fraudsters either online, by phone, mail or in person. Weaknesses in the eligibility assessment process means that ineligible persons could obtain a Seniors Card and receive payments and benefits for which they are not entitled.

The Department is improving its management of the Seniors Card system. A review of the Seniors Cards terms and conditions is also underway to ensure that only eligible Seniors Card holders receive benefits.

[4] On 1 July 2015, the age criteria for new WA Seniors Card applications will change. New applicants must be at least 61 years old to be eligible. The age eligibility for the WA Seniors Card will increase by one year every two years to 65 years old by 2023-24. Existing Seniors Card holders will not be affected by the change.

Key findings

The integrity of the system is at risk from false or inaccurate information

The Department does not routinely check the accuracy of information contained in Seniors Card application forms. The entering of false and inaccurate information into the system could lead to inaccurate records, and to the issue of Seniors Cards to ineligible applicants.

The Department accepts applications by post, email and in person. The applications are required to include some form of identification, though copies of identification documents are accepted. Identification can include a Driver's Licence, Aged Pensioner Concession Card, Passport, Birth and Marriage Certificates or Proof of Age Card.

As copied identification is not certified, there is a real risk of the Department receiving false information from an applicant and of inappropriate concessions and rebates being made. We have raised this issue with the Department for some years and have 'qualified' our opinion on their financial statements. However, the Department is addressing the risk with a new requirement that from 1 July 2015, all new applicants must satisfy a 100 point identity check.

We have also been concerned for some years about the lack of any validation of claims by applicants that they work less than 25 hours a week averaged over a year and that this ongoing requirement is met in the years following the granting of a card.

Before implementing the new system in May 2014, the Department had to transfer information from the old system to the new. During this process, it did not try to detect and correct corrupt or inaccurate records by using data cleansing. In addition, it could not load some historic unknown payment information into the new database. This means that these payments cannot be reconciled as the information is not readily available.

Security of senior's personal information needs improvement

The database for the Seniors Card system had a number of security weaknesses. This database holds sensitive information for seniors, including their full name, date of birth, address, contact numbers and bank account details, so it is important to keep it secure.

Some of the weaknesses we noted were:

- **Passwords are not changed often enough** – There is no policy that requires staff to update passwords regularly. For example, we saw one administrator password that was over a year old. This increases the risk that it will become known and misused. If someone did acquire the password, enforcing regular password updates limits the period they are able to use it for malicious purposes.
- **Database access and changes are not recorded** – The Department does not track any database access and changes. This makes it harder to detect unauthorised changes or access to sensitive information. If there was a breach the Department would not be able to track who accessed what information.
- **Basic security updates are not applied** – The database does not have the recommended security updates, which help to protect systems against cyber-threats and malware. To minimise the risk of known threats, security updates need to be assessed and applied in a timely manner.

Additional data stores increase the risk of information loss

The test and development environments within the Department contain the same data found in the Seniors Card system. This increases the risk that sensitive information will be compromised as these environments do not have the same security controls applied and the information they contain is available to individuals that may not need 'live' information.

The old Seniors Card system was decommissioned in 2014 but still contains a significant amount of personal information. A number of staff still have access to this application. The old system is not updated with the latest security patches. This creates an unnecessary risk of inappropriate access to this personal information.

Manual processes increase the risk of errors

The Department processes approximately 500 new application forms each week. Information from each of the Seniors Card application forms is entered manually into the system. A random sample of records are selected from the system each day for checking against the corresponding application form. A small number of errors are found during these checks. In addition, the system does not accommodate some formats of information, such as foreign certificates. This forces manual work arounds that may increase the risk of incorrect information in the system.

The Seniors Card system requires information to be exported and sent to a third party application on a dedicated computer before cards can be printed. During the audit, we noted that users logged onto this computer using a generic account and that the login details were attached to the keyboard. The Department immediately removed the login details when we brought it to their attention. Nevertheless, this manual process and use of a generic account does create a risk that unauthorised or unintentional modification or misuse of the system and key data may occur.

When producing reports for management, staff collect information from the Seniors Card and phone system to create reports using spreadsheets. This process requires several staff and is labour intensive. The manual compilation of reports is inefficient and increases the risk of input errors, affecting the reliability of reporting. Unreliable reports increase the risk that management make incorrect decisions based on this information.

The Department is currently reviewing these processes and are planning to automate them where appropriate.

Recommendations

1. **By the end of 2015, the Department of Local Government and Communities should:**
    a) **collaborate with agencies that can verify card applicant's information, to ensure the correct information is captured and processed**
    b) **ensure appropriate access controls are in place and maintained across all environments containing senior's information**
    c) **apply security updates to systems in a timely fashion**
    d) **consider how to best use their reporting function to prepare suitable reports for Seniors Card information.**

Agency response

The Department of Local Government and Communities accepts the Auditor General's Summary of Findings in relation to the WA Seniors Card System, noting that a number of these findings were in the process of being addressed.

The department has taken steps to strengthen the integrity of the system, including the verification of card holder details against databases held by the Western Australian Electoral Commission and the Department of Transport. This led to the suspension of unverified card holders. The department has also strengthened the certification and validation of applicant information to prevent risk of false or inaccurate information.

The department is reviewing the criterion relating to working hours and its implementation.

Upon assuming responsibility for the system after the audit, the department has addressed the findings in relation to information security by applying and maintaining security and software updates, deleting old systems and encrypting backups. Current security protocols have been maintained and generic accounts deleted.

The department is developing a new Seniors Card web portal, with applicants entering their data directly through the new portal. This will eliminate the need for manual processing. The new web portal will ensure data integrity, data privacy, and meet audit and management reporting requirements.

The Department of Local Government and Communities is committed to the continued improvement of the Seniors Card System.

Services Information Management System 2 – Drug and Alcohol Office of Western Australia

Background

The Drug and Alcohol Office[5] (DAO) plays an important role in the prevention, treatment, education and training and research into drug and alcohol consumption across Western Australia.

DAO's treatment and counselling services means that it collects confidential information regarding medical diagnosis, treatment and prescriptions. Staff use paper based client records, and later transfer this information to an application that manages and records this sensitive information.

In 2010, DAO released a new version of the application, known as Services Information Management System 2 (SIMS2). DAO developed the application in house, closely modelling it on DAO's existing processes and work practices. Key stakeholders have reported that the application suits their needs. The application holds records of approximately 240 000 clients across the state who are dealing with drug and alcohol issues.

DAO's role in managing its clients requires some staff to have access to the SIMS2 application. This includes doctors, nurses, psychologists and pharmacists. Securing this information is an important obligation on DAO.

DAO are also required to submit data to the Australian Institute of Health and Welfare (AIHW) as part of the Alcohol and Other Drug Treatment Services National Minimum Data Set (AODTS NMDS). SIMS2 allows DAO to ensure that the mandatory reporting data is collected and accurate. The AIHW use this data to report annually on Alcohol and other drug treatment services in Australia. Information from these reports helps to inform national strategies on drug and alcohol abuse.

Audit conclusion

SIMS2 assists DAO to record client information and perform its core business efficiently. The ability to access client information readily and store records electronically helps staff to manage client's needs.

However, inadequate access and other security controls over confidential client information leaves the system vulnerable to improper disclosure.

DAO could also improve its server room environment and disaster recovery testing to minimise the risk of system outages and ensure ongoing operations.

Key findings

Security of electronic client records

There is inadequate protection of sensitive client information in the SIMS2 database and DAO lacks the controls needed to recognise when unauthorised access has occurred. The database includes medical information for clients including their full name, date of birth, address, contact numbers, full treatment history and medication details. Without appropriate database controls

[5] The Drug and Alcohol Office and the Mental Health Commission amalgamated on 1 July, 2015. The joined organisation is called the Mental Health Commission.

and system security, there is an increased risk of unauthorised disclosure or misuse of client information.

Some of the weaknesses we noted were:

- **Access and logging of reports** – DAO does not have policies or procedures that determine which system reports can be generated and by whom. All staff, regardless of their role have access to confidential client information through the SIMS2 reporting functions. DAO does not log who runs reports or their SIMS2 download activity. This means DAO cannot detect improper access to the information. For example, a staff member could export client records and save or store these to external devices without DAO's knowledge.
- **IT team access is unrestricted** – Information in SIMS2 is copied between the test, production and live environments of the application. This means that the IT team members had broader access to the information than is needed. IT staff were able to read, delete or alter the client history and information undetected across all environments.
- **System security** – Essential security controls are not in place. For example, we found weak passwords for accessing the database and multiple temporary accounts. DAO does not install the recommended security updates to the SIMS2 database to help protect its confidential information from cyber-threats and malware.

Controls to ensure ongoing operations

DAO has identified SIMS2 as critical to their day-to-day functions. If SIMS2 is unavailable for longer than 24 hours, client treatment may be impacted. DAO has developed IT Disaster Recovery Plans to restore service operations in the event of a serious incident. However, DAO has not tested these plans since 2010 to ensure they are still suitable.

We also found some opportunities to reduce the risk of a SIMS2 outage when we reviewed the maintenance of server rooms and supporting equipment:

- DAO uses its server rooms for other activities such as CCTV monitoring and building of computers. Undertaking these activities near critical servers and equipment together with untidy network cabling enhances the risk of disruptions.
- The server rooms did not have monitors to alert IT staff during or after business hours of changes in the environment that may affect a server, such as an air conditioner malfunction.

Recommendations

1. **By June 2016 the Drug and Alcohol Office should:**

    a) **ensure it has the appropriate controls in place to limit the risk of information loss from their network**

    b) **identify vulnerabilities and apply updates within a timely manner within the SIMS2 and supporting IT infrastructure**

    c) **improve the computer room environment to minimise the risk of system outages and conduct IT Disaster Recovery Plan testing as required.**

Agency response

The Mental Health Commission (MHC) acknowledges the findings of the applications controls review. The audit process has highlighted a number of issues and work is ongoing by the MHC to improve the infrastructure, process and controls in place.

A number of items identified in the audit have already been addressed and the remainder will be finalised, as per your recommendation, by June 2016.

Appendix 1: Guidance on database security

Introduction

To begin adequately securing their databases, agencies should assess the value of data stored within them. This data may be personal, commercially sensitive, a target for fraud, or protected under legislation. Agencies should fully understand the consequences of data disclosure, theft or tampering to ensure they expend appropriate effort on security controls.

When considering applying data security controls, it is important to consider where else the data in a production environment may reside. These may include:

- Test, Development or Training environments

Where possible, these systems should use anonymised or masked data. If it is essential that production data is used, even if it is old data, the databases should be secured to the same level as the Production system. Development or Test systems may be less hardened and host potentially insecure services, so additional network segregation may be required.

- Other systems such as reporting or staging databases

Other systems within an agency may need to extract and process sensitive data for a variety of purposes. In these instances, the minimum required data should be extracted to address requirements. Access restrictions, password security and account settings present in the primary database should be applied consistently across these additional systems.

- Backups and disaster recovery images of the production database

The production database should be backed up and replicated, to allow for recovery in the event of a disaster. Any replicated copies or versions of the database should be secured to the same level as the production system. Agencies should conduct a risk assessment on the storage of backup images or media. This should include the physical storage or external media, and may include encryption backups.

Account security

The accounts used to access databases must be well controlled and secured. All database user accounts, regardless of their purpose, require a strong password. The passwords used by general users should conform to good practice for complex, hard to guess passwords. These passwords should be set in line with agency password policies and standards. Passwords for administrators and other highly privileged users should be more complex, to reflect the risk presented by a compromised account.

Service and System accounts should be used only by automated services and process, not by individuals. Agencies should consider changing these passwords periodically, and when administrators with access to these accounts leave the agency.

To enable accountability and auditing, administrators should utilise their personal accounts where possible. The passwords for user and administrator accounts should expire periodically.

Systems should be configured to automatically lockout user accounts after a set number of incorrect attempts. This can defeat attempts by an attacker to either guess the password or to use an automated tool to crack the password using ‘brute force’.

The attributes of a hard to guess password include:

- sufficient characters
- a mix of alphanumeric and 'special' characters
- do not contain the username, the name of the application or the agency name
- does not contain common dictionary words (e.g. password, test, welcome) or patterns (e.g. qwerty, 12345, abcde)
- has not been used on that system previously by that user.

Password advice for high security environments is available from the Australian Signals Directorate Information Security Manual[6] (ASD ISM).

Database accounts should be periodically audited and examined to see if they:

- are still required
- are assigned appropriate access rights and privileges.

This process ensures that:

- access is revoked for users that have left the agency
- access is modified or revoked for users that have changed roles within the agency
- accounts belonging to obsolete services, or allocated for short term initiates, are removed
- accounts that have not been used for extended periods are assessed
- possible 'rogue' accounts that have been created without authorisation (possibly by an attacker) are discovered and removed.

These alterations should be made at the time of the role change or termination, with audits acting as a follow-up assurance process. An attacker may also seek to create a new account to maintain access to a database without disrupting a normal user. Regular audits will aid in the detection of any 'rogue' accounts.

Version and patches

Database software, and its supporting operating systems, should be patched and upgraded regularly. Agencies should include databases in their wider patching and vulnerability management programs.

Patches, service packs and upgrades issued by the vendor should be risk assessed and installed on Test or other Pre-Production environments before installation on live systems. This reduces the risk of any complications or issues arising from a patch. This process should be handled as per agency Change Control procedures.

Agencies may also wish to use a Vulnerability Scanning tool to seek assurance that their patching program is effective. These tools are also effective to ensure that systems remain

[6] Pages 189 to 193 http://www.asd.gov.au/publications/Information_Security_Manual_2015_Controls.pdf

patched after restores from backup or major configuration changes, and are not vulnerable to newly disclosed vulnerabilities.

Database software and operating systems will also undergo significant version changes and upgrades over time. Agencies should keep pace with version changes to ensure that their implementations are supported by the software vendor. Over time, vendors may stop supporting software, meaning that patches (including security patches) will not be released and technical support will not offered. While it may be possible to enter into a custom support arrangement, this will come at a heavy financial cost.

Where databases cannot be quickly patched or upgraded to new versions compensating security controls should be applied. This may include additional physical or logical network segregation and increased monitoring. It is important that the risks posed by out of date systems are assessed on a regular basis. Examples of compensating controls are included in this document under Attack Surface and System Hardening.

Additional advice on system patching and vulnerability management is available from the ASD, both in the ASD ISM and at a high level from the Cyber Security Operations Centre.

Attack surface

Minimising the available Attack Surface reduces the opportunities for an attacker to exploit weaknesses in a database. Any unused or un-configured databases schemas, features or services should be removed.

Guides available from the Centre for Internet Security provide detail on how to remove unnecessary software components from newly deployed systems[7].

Database servers should be segregated from the rest of the network, with rules allowing only necessary services and ports to be exposed to end users. This reduces the exposure of other management services and interfaces that may be vulnerable to attack.

Segregation of the internal network (beyond just segregation from the internet) will increase the effort the difficulty, or 'cost', to an attacker seeking to access sensitive data and systems.

Some administrators will require additional access to databases to perform administrative tasks and troubleshooting. These workstations should be limited in number and have additional security controls, such as monitoring, applied. Agencies may consider the use of 'jump servers' or 'jump hosts' that allow administrators remote access to a general use system within the same network segment as the database.

System hardening

The configuration of a newly installed database can be insecure and should be hardened.

Post installation tasks include:

- restrict default access rights and permissions, particularly 'PUBLIC' access
- change default passwords
- remove built-in user accounts that are not required
- align configuration settings with the IT environment and system requirements.

[7] http://www.asd.gov.au/publications/protect/Assessing_Security_Vulnerabilities_and_Patches.pdf

Detailed hardening guides that conform to good practice are available from the Centre for Internet Security 'Security Benchmarks' program.[8]

Data protection

At the database level, data protection[9] can be achieved by:

- encryption of the database, or certain records within it
- use of Virtual Private Databases to apply explicit security restrictions with database tables
- redaction of sensitive data. This may include highly sensitive personal information or credit card numbers.

As mentioned above, any data protection controls applied within the primary database should be replicated within any other copies or instances of the data.

Backdoors/misconfiguration

If databases and their underlying operating systems are misconfigured, sensitive data or system settings can be exposed to unauthorised users. Before deploying a new system into a production environment, the configuration should be checked against best practice recommendations and tailored to the purpose of the system.

Agencies may wish to engage specialists to review and test database configurations before deploying a system or after significant changes occur. A robust Change Control process, supported by policy and documented procedures, should be used to ensure that any modifications to the production environment are properly planned, tested and endorsed.

An attacker may also alter the system configuration to open a security hole, or back door, allowing them to maintain access to data during a prolonged attacked. Such an alteration could be considered an unauthorised change. Agencies that apply suitable detective controls, such as auditing and logging, may be able to detect these changes.

Auditing/monitoring

Databases should be configured to log and store sensitive actions performed by users, and the system itself. The nature and detail of this logging will differ from system to system, depending on agency requirements.

Process should be established to monitor and to audit logs for suspicious behaviour or another anomalies. Logging should contain, amongst other items:

- successful and rejected login attempts
- account lockouts
- account administration tasks:
    - account creation and deletion
    - password changes

[8] https://benchmarks.cisecurity.org/
[9] https://benchmarks.cisecurity.org/

    - user rights and role changes
    - account locks and unlocks
- execution of queries (SELECT, UPDATE, DELETE and INSERT) for sensitive data
- changes to system configuration.

Log data should be adequately protected against unauthorised deletion and modification to ensure its integrity and reliability. Automatically duplicating or sending logs to a separate logging system may be advisable in some environments. This allows for more stringent access control to be applied, particularly to accounts that have high levels of privilege to a database and/or operating system. Logs stored in a secondary location also allows for a level of redundancy in logging if the primary system is compromised or destroyed.

Processes should be developed to review and audit logging data once it has been collected. Agencies should use their prior assessments of sensitive data and high risk activities to guide log reviews. If possible, segregation of duties should be introduced to ensure that administrators are not the only party to audit systems under their control.

Additional advice on good practice for database auditing is available from the Centre for Internet Security, referenced above. General advice on logging is available in ISO/IEC 27002:13.[10]

[10] ISO/IEC 27002:13 12.4 http://www.iso.org/iso/catalogue_detail?csnumber=54533

Auditor General's Reports

Report Number	Reports	Date Tabled
22	Safe and Viable Cycling in the Perth Metropolitan Area	14 October 2015
21	Opinions on Ministerial Notifications	8 October 2015
20	Agency Gift Registers	8 October 2015
19	Opinions on Ministerial Notifications	27 August 2015
18	Controls Over Employee Terminations	27 August 2015
17	Support and Preparedness of Fire and Emergency Services Volunteers	20 August 2015
16	Follow-On: Managing Student Attendance in Western Australian Public Schools	19 August 2015
15	Pilbara Underground Power Project	12 August 2015
14	Management of Pesticides in Western Australia	30 June 2015
13	Managing the Accuracy of Leave Records	30 June 2015
12	Opinions on Ministerial Notifications	25 June 2015
11	Regulation of Training Organisations	24 June 2015
10	Management of Adults on Bail	10 June 2015
9	Opinions on Ministerial Notifications	4 June 2015
8	Delivering Essential Services to Remote Aboriginal Communities	6 May 2015
7	Audit Results Report – Annual 2014 Financial Audits	6 May 2015
6	Managing and Monitoring Motor Vehicle Usage	29 April 2015
5	Official Public Sector Air Travel	29 April 2015
4	SIHI: District Medical Workforce Investment Program	23 April 2015
3	Asbestos Management in Public Sector Agencies	22 April 2015
2	Main Roads Projects to Address Traffic Congestion	25 March 2015
1	Regulation of Real Estate and Settlement Agents	18 February 2015

Office of the Auditor General
Western Australia

7th Floor Albert Facey House
469 Wellington Street, Perth

Mail to:
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

Follow us on Twitter @OAG_WA

Download QR Code Scanner app and scan code to access more information about our Office