Western Australian
Auditor General’s Report

Information Systems Audit Report 2018

Report 1: August 2018-19

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)

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

ISSN: 2200-1931 (Print)
ISSN: 2200-1921 (Online)

WESTERN AUSTRALIAN AUDITOR GENERAL’S REPORT

Information Systems Audit Report 2018

Report 1
August 2018-19

WESTERN AUSTRALIA

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

INFORMATION SYSTEMS AUDIT REPORT 2018

This report has been prepared for Parliament under the provisions of section 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.

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

CAROLINE SPENCER
AUDITOR GENERAL
21 August 2018

Contents

Auditor General's overview

This is the tenth annual *Information Systems Audit Report* by my Office*.* The report summarises the results of the 2017 annual cycle of audits, plus an examination of passwords and application reviews completed by our Information Systems audit group since last year's report.

The report is important because it reveals the common information system weaknesses we identified that can seriously affect the operations of government and potentially compromise sensitive information held by agencies. It also contains recommendations that address these common weaknesses and as such, has a use broader than just the agencies we audited.

Common weaknesses across all our information systems audits indicate agencies are not taking risks to information systems seriously enough. Most of the issues raised can be easily addressed and it appears that risks are simply not properly understood. They are certainly not being effectively managed.

The first section in my report shows that agency systems are vulnerable as a result of weak passwords. We have demonstrated to agencies on many occasions how weak passwords are used to access information systems without detection. A pressing issue that must be acknowledged and addressed across the sector is for agencies' executive management to engage with information security, instead of regarding it as a matter for their IT departments. The days of senior leaders not understanding information security and capability as a key business risk to be closely monitored and appropriately managed are over. The consequences to state service delivery, trust in the sector and institutional reputations are too great.

Our applications reviews show that agencies also need to take the initiative and perform their own reviews to identify critical controls, inefficiencies and problems and potential solutions. An analysis of people, process, technology and data relevant to key IT applications would help management identify and manage risks.

In the third section of this report, I have identified 2 agencies that have consistently demonstrated good system management controls. Our results show improvements were made in 2017 across most areas. However, information security and business continuity remain a concern with only half or less of agencies performing to the expected level.

Password Management in the WA State Government

Introduction

Western Australian government agencies collect and store a significant amount of sensitive and confidential information. The public rightly expects agencies to protect this information from unauthorised access. Effective management and use of passwords remains a vital part of information security. However, since 2004 our information systems audits have consistently raised issues around agency access controls, particularly passwords.

The objective of this audit was to determine if selected government agencies are using good practices to manage network passwords, to protect the information they hold.

Conclusion

Over one quarter of the enabled network accounts we looked at had weak passwords at the time of audit. In a number of instances these accounts are used to access critical agency systems and information via remote access without any additional controls.

Generally, agencies lacked technical controls to enforce good passwords across networks, applications and databases, and did not have guidance about good practice for password management.

Background

Agencies have a diverse range of users, applications and services with different purposes and security requirements. These require different types of accounts or identities to access information from inside and outside agencies. For example:

- Employees: Normal user accounts for staff to perform day-to-day tasks
- Partners: contractors and vendor support staff
- Privilege Accounts: Individuals with high level administrative privileges such as system, network and database administrators
- Shared and Generic Accounts: Default accounts and vendor accounts that are not specific to an individual and where passwords are shared with other users
- Services and Applications: Accounts used by operating system services and applications such as web servers, email services and backup accounts.

Passwords are still the main control agencies use to protect information systems and are an important security mechanism for all account types. Good password management practices combine people, process and technology to secure the use and management of passwords. Creating complex, hard to guess passwords requires at least 3 of the following categories:

- uppercase
- lowercase
- digits (0 through 9)
- non-alphanumeric characters (e.g. !, $).

However, passwords that meet complexity requirements, may still be considered weak if they use common variations of words or keyboard patterns or are included in publicly available password dictionaries.

The importance of password security is well known. The July 2018 *Notifiable Data Breaches Quarterly Statistics Report*[1] stated that 59% of data breaches involved malicious attacks, with most the result of compromised credentials. Phishing and brute force accounted for 43% of the attacks. Another global report[2] linked 81% of hacking-related breaches to stolen or weak passwords. Globally it is estimated that each data breach cost an average of US$3.62m[3].

What we did

As part of our annual information systems audits, we assessed 17 agencies' processes and controls in place to manage passwords and privileged accounts. We processed about 520,000 enabled and disabled accounts across agencies' Active Directory (AD) environments by collecting the AD information using encrypted USBs. We analysed and disposed of the information in a secure offline environment. In performing this work, we:

- assessed encrypted passwords from each agency's AD environments. We also assessed old disabled accounts to understand password composition trends over time. Where possible, we used data from the AD to determine the account purpose and level of privilege for each of the accounts
- used a password cracking method known as Dictionary Attack and a list of well-known or commonly used passwords such as 'Password1' and 'Welcome123'. We compiled the list from publicly available password dictionaries used for penetration testing assessments. Weak passwords not on our list were not identified as part of our testing
- reviewed agency policies and security awareness training
- provided agencies with information so they can implement strong passwords for identified weak accounts.

[1] https://www.oaic.gov.au/resources/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics/notifiable-data-breaches-quarterly-statistics-report-1-april-30-june-2018.pdf
[2] https://www.verizonenterprise.com/resources/reports/2017_dbir_en_xg.pdf
[3] https://www.ibm.com/security/data-breach

Audit findings

More than one quarter of the enabled accounts we assessed had weak or commonly used passwords

We reviewed approximately 234,000 enabled accounts across 17 agencies and 23 AD environments. Of these, 26% (60,000) had weak or commonly used passwords. Weak passwords increase the risk of successful cyber-attacks with hackers gaining unauthorised access to systems and information.

Without adequate password controls in place the overall security of systems is potentially reduced increasing the risk of unauthorised access, as can been seen in the case study below.

Easily guessed password for internet accessible system

In 2017, we assessed a test environment from a WA agency's web system, which was publicly available through the internet. We gained access to the agency's network with full system administrator privileges by using an easily guessed password, Summer123. We identified a significant amount of production data in this environment.

Figure 1: Potential risk of using easily guessed passwords

Table 1 shows the top 20 weak passwords across our sample agencies. These passwords were used in 6,546 enabled accounts.

No.	Password used	Accounts
1	Password123	1,464
2	Project10	994
3	support	866
4	password1	813
5	October2017	226
6	Monday01	225
7	Spring17	198
8	Sunday01	188
9	password	184
10	abcd1234	176
11	Spring2017	155
12	password2	142
13	August2017	141
14	sunday1	132
15	Welcome1	132
16	Password01	118
17	Summer01	102
18	Logitech1	98
19	support1	96
20	Summer17	96

Source: OAG

Table 1: Weak passwords we found most often

Many of these passwords comply with industry standards for password complexity and a length of at least 8 characters. This indicates that merely applying these parameters is insufficient to guard against inappropriate access to networks and systems.

Table 2 shows the 10 agencies in our sample with the highest percentage of weak passwords. Between 20% and 56% of enabled accounts in these agencies, were found to have weak passwords. This included over 400 privileged accounts which, because of their level of administrator access, pose a higher risk of unauthorised access to data.

Agency	% of weak passwords	Privileged accounts with weak passwords
1	56	3
2	49	5
3	43	90
4	41	5
5	39	250
6	38	28
7	32	12
8	27	1
9	22	7
10	20	18

Source: OAG

Table 2: 10 agencies with highest percentage of weak passwords

We also looked at 5 common patterns used to create passwords. Our results are shown in Table 3. In ‘Variants of date and season’, we looked for passwords containing days of the week, months, season and years between 1900 and 2050. For ‘Variants of qwerty’, we looked for passwords that contain ‘qwe’.

Patterns	Enabled accounts using pattern	% of total weak passwords
Variants of date and season	12,744	**21.28**
Variants of ‘123’	6,827	**11.40**
Variants of word ‘password’	5,182	**8.65**
Only digits	765	**1.28**
Variants of ‘qwerty’	47	**< 1**

Source: OAG

Table 3: Use of 5 common password patterns

Recent published lists of worst passwords still show variations of the word ‘password’, the keyboard pattern ‘qwerty’, and passwords that contain only digits as the most used patterns. Our review of WA agencies has confirmed this.

Agency passwords are longer, but still weak

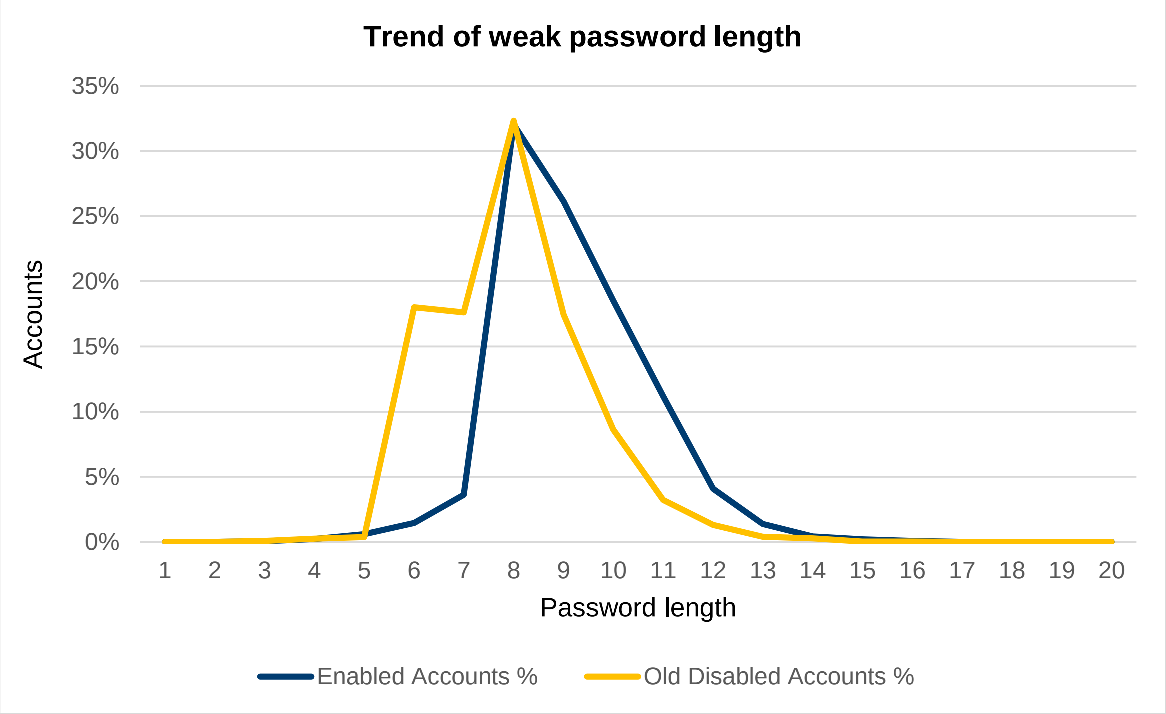
Password length is one of the most advocated mitigation strategies for increasing password security. We assessed the length of weak passwords, in both disabled and enabled accounts, across the 17 agencies. We found that even weak passwords were generally of reasonable length. A summary of our findings is presented in Table 4.

Password length	Accounts	%
1	6	0.01
2	6	0.01
3	63	0.06
4	226	0.23
5	494	0.50
6	7,696	7.80
7	9,117	9.24
8	32,086	32.51
9	22,267	22.56
10	14,353	14.54
11	7912	8.02
12	2,934	2.97
13	977	0.99
14	357	0.36
15	130	0.13
16	55	0.06
17	7	0.01
18	5	0.01
19	2	0.00
20	2	0.00

Source: OAG

Table 4: Weak password length

Figure 2 shows our comparison of weak passwords across disabled and enabled accounts. Eight characters is the most used password length for both types of accounts and most enabled accounts (88%)[4] have passwords between 8 and 11 characters. Agencies are using longer passwords, but they are still weak. Although longer passwords are generally considered better, easily guessed long passwords do not adequately mitigate the risk of unauthorised access to systems.



Source: OAG

Figure 2: Length of weak passwords

[4] 998 accounts did not have the enable/disable status identified.

Password complexity requirements are in place, but not enforced

All agencies in our sample have password complexity requirements configured in their AD for network access. However, enabled accounts were not always forced to renew their passwords and complexity requirements were only enforced when passwords were created or changed. Several existing accounts still had simple passwords.

Our audit showed that 13% (7,633) of the agencies systems, services and user accounts do not comply with agencies' password policies or complexity settings. Additionally, we found many accounts were set to never request password changes.

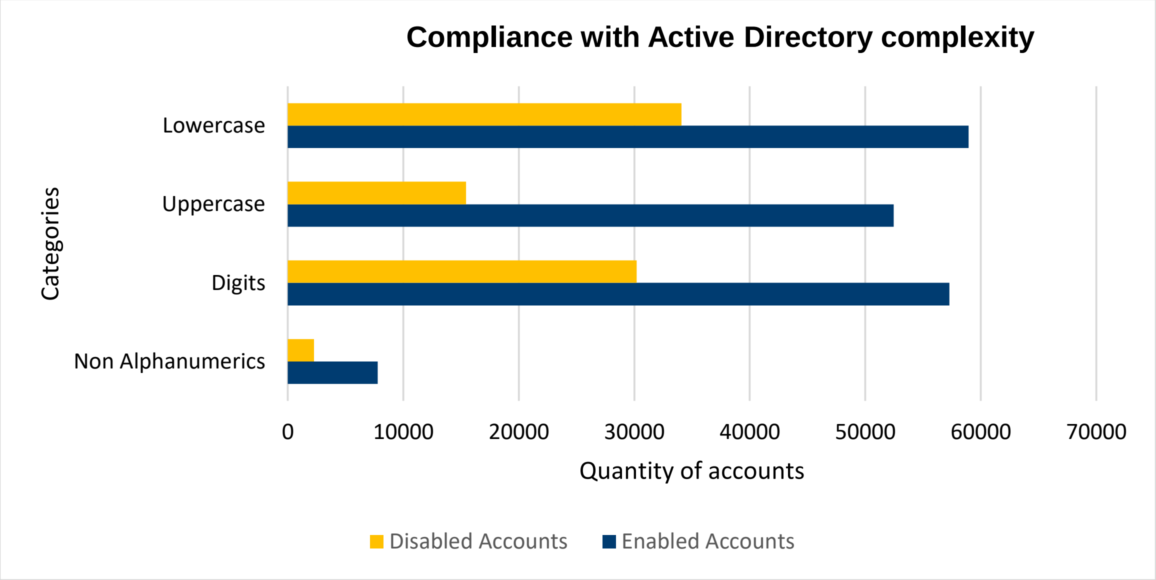
Table 5 shows the percentage of enabled accounts that comply with password complexity requirements. However, as can be seen from Table 1, weak passwords can also meet the complexity requirements. Agencies need to do more to mitigate the risk of passwords being comprised, such as blacklisting commonly used passwords.

Result	Contain uppercase	Contain lowercase	Contain digits	Contain non alphanumeric	Comply with basic AD complexity
Yes	88%	98%	96%	13%	87%
No	12%	2%	4%	87%	13%

Source: OAG

Table 5: Compliance with complexity requirements – enabled accounts

Our comparison of enabled and old disabled accounts shows newer accounts have a higher levels of compliance with basic AD complexity requirements (Figure 3). This may reflect improvements in how agencies are managing and enforcing AD complexity requirements.



Source: OAG

Figure 3: Compliance with password complexity – enabled and disabled

Password policies and controls are inadequate and do not address different security risks

We found that agencies password management and access control policies are not comprehensive. Policies do not tailor security requirements to different identities (e.g. people, application, services) and endpoints (on and off premises, mobile, cloud) within their environments.

One agency had not implemented any password policy and controls for their internet accessible application, which is used by the WA business community and members of the public. Without appropriate management of passwords there is an increased risk that unauthorised or unintentional modifications of IT systems will occur. This could impact the confidentiality, integrity and availability of agency information.

Agency staff need more support and remote access systems are vulnerable

We found most agencies do not guide or support users to securely store and manage passwords. Users need to remember dozens of personal and work-related passwords and may write them down in spreadsheets or Word documents.

To reduce the need for multiple passwords or to lessen the risk of users mismanaging their passwords, some agencies have:

- implemented single sign-on (SSO)
- used multi-factor authentication
- provided users with online or offline password managers to securely store their passwords.

At least 12 of the 17 sampled agencies did not have multi-factor authentication as an additional layer of security for key systems that are accessible via remote access. Relying only on passwords leave these key systems vulnerable to attacks and increase the risk of unauthorised access. This risk was realised in 2017 when North Metropolitan TAFE reported a hacker had gained unauthorised remote access to their network and encrypted password hashes.

Agencies do not understand Active Directory security risks

The AD database contains significant amounts of information regarding user accounts and the network. We found that agencies do not generally monitor access and changes to this database. We also found:

- One agency had old offline versions of the AD database stored on the server and widely available to IT support users and contractors. This information would provide an attacker with the information they need to obtain unauthorised access to the agency's accounts and network without the agency knowing.
- Another agency inadvertently shared its entire AD database with a third party. The database contained all user account information including staff names, usernames and encrypted passwords. This has left the agency exposed to unacceptable risks.

Privileged accounts are not appropriately managed, increasing the risk of security incidents

Administrator accounts are not well managed

Most agencies do not have effective security controls in place to manage privileged identities and access. We identified over 460 enabled privileged accounts with weak passwords. All agencies we reviewed had at least 1 privileged account with a weak password, with 1 agency having 250 accounts. Even larger agencies, which we expect to have good practices to protect their information assets, were found to have privileged accounts with weak passwords.

Privileged accounts present a high risk because of their level of administrative access. For this reason, restricting privileges is included as one of the Australian Signals Directorate's

(ASD) Essential Eight strategies of practical actions that agencies can take to make their computers and networks more secure.

However, we found most agencies are not managing privileged identities and access appropriately. None of the agencies we reviewed had established Privileged Identity Management or Privileged Access Management to centrally control access to privileged accounts, or included the need for one in their planning.

Privileged system, service and application accounts are neglected

Agencies generally neglect the importance of high privileged system, service and application accounts and do not manage them appropriately. This is despite these being among the most targeted by hackers because they allow the user to increase the privileges attached to an account.

We found many of these accounts with weak passwords across all agencies. One agency, not referred to in Table 2, had 180 systems and services accounts with weak passwords. Also, 1 account with domain administrator privileges, used for backup services, had not had its password changed for 14 years. This level of privilege has full access to change the network domain.

Further, most agencies do not keep sufficient information on these privileged accounts to determine their purpose. Consequently, agencies are not fully aware of what these accounts are used for and are reluctant to disable the accounts or change the passwords.

Accounts shared with multiple users increase the risk of unauthorised access

Generic and shared accounts violate the principle of 'least privilege'. This is where only required privileges to complete the specific work should be granted, and accountability assigned to a specific user. One agency had over 2,000 of these accounts. The accounts generally have shared passwords and limited ability to track actions back to individuals and therefore present a high risk of unauthorised access.

We identified issues with these types of accounts during our 2017 General Computer Controls audit cycle. Common issues reported to agencies were:

- accounts using weak passwords
- lack of formal process for requesting, approving and managing the accounts
- no centralised register/inventory with a description of purpose and who is responsible for the use of the account
- high privileged generic and shared accounts used for remote access
- accounts belonging to terminated employees or partners that retain access to systems and data centres.

Recommendations

1. The Department of the Premier and Cabinet should:

   a. provide guidance to agencies on ways to better manage identities and access including password management and multi-factor authentication

      DPC response: Agreed

      Implementation timeframe: by 31 December 2018

2. All agencies should:

   a. have adequate security policies in place that require a lifecycle management approach for different types of accounts and access levels

   b. implement privileged identity and access management best practices

   c. consider providing staff with a secure way of storing passwords and technical solutions to reduce the number of passwords users need

   d. use multi-factor authentication for remote access

   e. prevent/blacklist the use of common weak passwords

   f. tailor password requirements for each type of account, based on the risk, environment (e.g. On-premise, Cloud) and other mitigating controls in place

   g. maintain visibility on the purpose, ownership and use of service, system and database accounts.

Agency response

DPC agrees with the recommendations detailed in the Summary of Findings. The Office of Digital Government (formerly Office of the Chief Government Information Officer) was transferred to the Department of the Premier and Cabinet (DPC) as a discrete business unit on 1 July 2018, to provide a stronger mandate for the Government's digital transformation agenda, and to ensure that ICT performance, data sharing and cyber security are strengthened. Since then, DPC has commenced recruitment for a new Government Chief Information Officer, as well as other cyber security positions, to support this mandate.

Since the audit, DPC has:

- provided advice to Directors General and Chief Executive Officers at the Public Sector Leadership Council, and through the CEO Gateway, on the impending release of the report, strongly encouraging agencies to take a number of practical actions to improve security, risk management and recover capabilities. This advice included encouraging agencies to review their practices and policies to ensure they are compliant with the Australian Signals Directorate Checklist.
- offered support to assist agencies with their cyber security matters through the Office of Digital Government.
- engaged with the 17 agencies named in the report and requested a status of their progress with implementation of the recommendations.
- organised a Directors General Cyber Security Forum for 29 August 2018, aimed at improving cyber security practices across government. The forum will bring together speakers from the Office of the Auditor General, DPC and Edith Cowan University.

Application Controls Audits

Introduction

Applications are software programs that facilitate an organisation’s key business processes including finance, human resources, case management, licensing and billing. Applications also facilitate specialist functions that are unique and essential to individual entities.

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

Audit focus and scope

We reviewed key business applications at 5 agencies. Each application is important to the operations of the agency and may affect stakeholders, including the public, if the application and related processes are not managed appropriately.

The 5 agency applications we reviewed were:

1. **Patient Medical Record System** – Department of Health
2. **Tenancy Bonds Management System** – Department of Mines, Industry Regulation and Safety
3. **First Home Owner Grant Online System** – Office of State Revenue
4. **Election Management System WA** – Western Australian Electoral Commission
5. **Keysmart System** – Keystart Housing Scheme Trust

Our application reviews look at the systematic processing and handling of data in the following categories:

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

Our testing of the above categories of controls is a point in time assessment. It is based on a sample of key controls and processes that are designed to obtain reasonable assurance about whether an application works as intended and that the information it contains and reports is reliable, accessible and secured. Our testing of some of those controls may highlight weaknesses in their design or implementation that increases the risk that an application's information may be susceptible to compromise. However, we do not design our tests to specifically determine whether information has been compromised.

Summary

All 5 applications had control weaknesses with most related to poor information security and policies and procedures. We also found issues with controls that aim to ensure the applications function efficiently, effectively and remain available. We reported 49 findings across the 5 applications with 9 of these rated as significant, 29 moderate and 11 minor.

Correcting most of the issues we raised is relatively simple and inexpensive. Figure 1 shows the findings for each of the areas and Figure 2 shows the findings for each of the 5 applications reviewed.

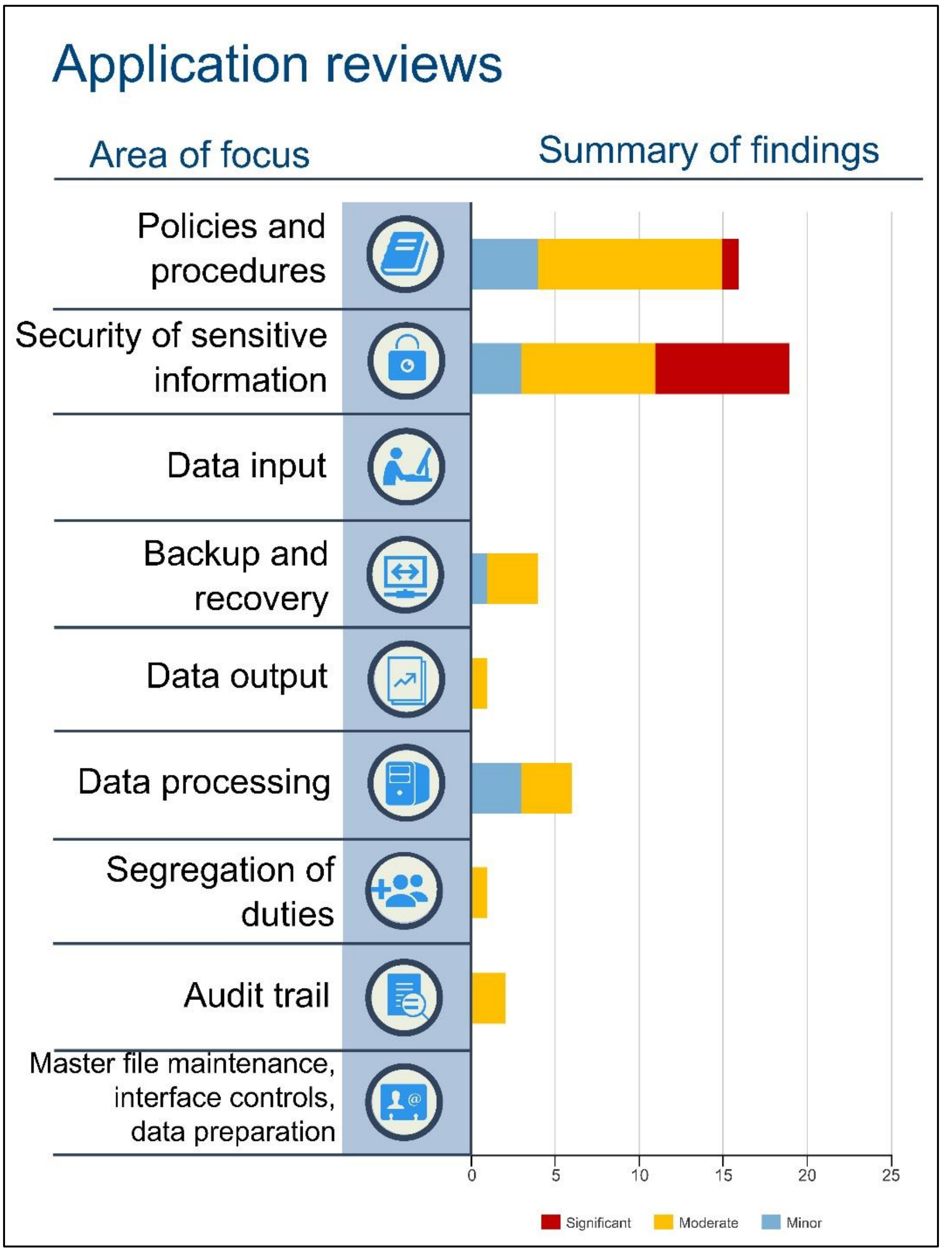


Figure 1: Application reviews

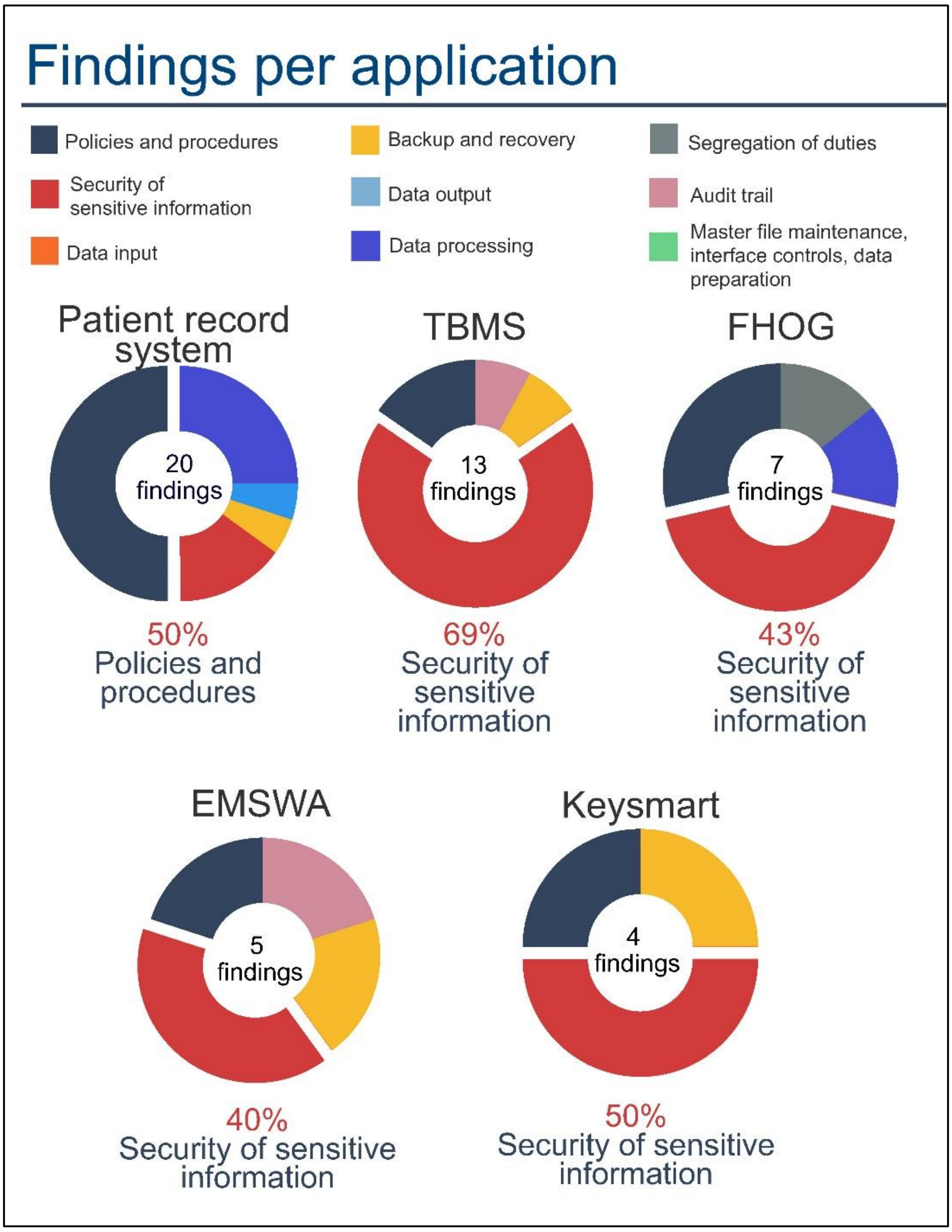
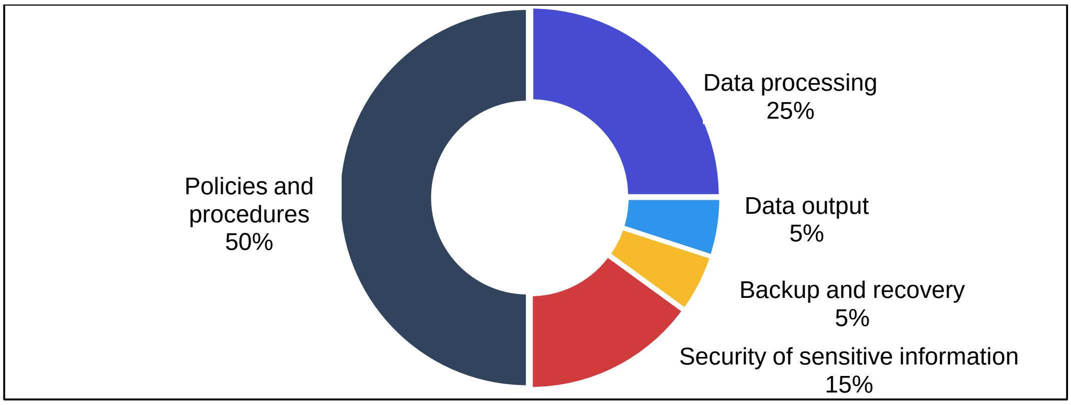


Figure 2: Findings per application

Patient Medical Record System – Department of Health



Introduction

Several Western Australian hospitals use a patient medical record system (the Application) to make patient medical records digitally available. This Application stores sensitive information such as patient identity and medical records.

Conclusion

The Department of Health (DoH) is still to decide if all medical health records will be digitised across Western Australia. This has impacted the realisation of expected efficiency gains and improvements in patient care records across the Health system from the implementation of the Application.

Poor contract management means the DoH does not know if the vendor is effectively delivering the Application and how it is tracking against the $20 million contract. To make fully informed decisions about its future use the DoH needs to understand the total cost of providing the application.

The Application allows users to store and access medical records for patients. However, there are multiple management issues, including manual workarounds and storage limitations, that have led to inefficient use of the Application. Security vulnerabilities also have the potential to expose confidential patient information to inappropriate access and misuse.

Background

A small number of hospitals across the Health system use the Application. It is used to create electronic progress notes during care and to scan paper medical records and store them, typically at the end of a patient's episode of care.

The Department of Finance procured the Application on behalf of the DoH. The vendor was awarded a contract for just over $20 million in total (including GST) in 2013. The contract was for an initial 5-year period with 2 options to extend for a total of another 5 years.

The procurement plan stated the anticipated objectives of the system were to:

- reduce reliance on and cost of maintaining paper records
- increase patient safety by providing rapid concurrent access to medical records
- streamline business processes by introducing more efficient record capture practices.

The Application has been deployed to varying extents at hospitals across the State including Bunbury, Busselton, Royal Perth, Fremantle and Fiona Stanley Hospital.

Health Support Services provide the infrastructure to support the Application across all hospitals.

Audit findings

Unclear decision-making and lack of digitisation strategy has impacted the implementation of the Application

A lack of strategic direction and operational oversight has impacted the efficient and effective implementation of the Application. The DoH is yet to decide if all medical health records will be digitised across Western Australia as they are still in the process of developing a digital strategy. As a result, decisions regarding the Application's design and deployment are made at individual hospitals without consideration of whole of Health needs. This increases the risk that the Application may not deliver against the stated objectives of:

- reduced reliance on and cost of maintaining paper records
- rapid and concurrent access to medical records
- more efficient record capture practices.

The Application provides digital access to historical medical records. Every patient has a paper file/record created which is scanned into the Application at the end of their episode of care. Efficiencies arise from having digital access to these records during subsequent episodes of care.

We found no evidence to show a reduction in the cost of maintaining paper records since deployment of the Application. To reduce the consumption rate of disk storage, medical records are being scanned at a resolution less than that required by the State Records Office to destroy the physical record. As a result, even after scanning, the DoH incurs costs to store physical records at an offsite storage location. This is inefficient, costly and contrary to the Application's stated objectives.

In addition, the Application's electronic storage consumption has greatly exceeded initial estimates, resulting in recurring system outages and additional costs. When storage limits are reached users are unable to access the system when treating patients and patient records cannot be scanned. This may cause a reliance on historical paper records and create a scanning backlog.

The DoH has not carried out a proper root cause analysis to identify and resolve the system outages. This is required to limit disruption to clinical workflows and enable informed decisions about future roll out strategies for the Application.

Lack of appropriate contract management means the DoH cannot be certain if it is on budget and getting what it paid for

The DoH does not know if the vendor is meeting the needs of the business or if contractual costs are being managed effectively. We identified weaknesses in how the DoH manages the vendor contract. In particular, lack of defined roles and responsibilities for managing the vendor, no routine reporting by the vendor and monitoring by the DoH staff of service level agreements, and no monitoring of contract costs.

In addition, the DoH does not know the total cost of providing the Application to the hospitals. The current $20 million contract does not include the cost of the hardware, vendor licences and support fees, staff resources responsible for scanning documents, and offsite storage of the original medical records. To make fully informed commercial decisions about contract extension the DoH needs to know the total cost of service performance of the Application.

We expected, but did not find, by May 2018 that the DoH had started to review future needs and whether to invoke the option to extend the vendor contract as the initial contract period is due to end in August 2018.

Manual processes could compromise the efficient use of the Application

We identified opportunities for the DoH to improve the use of the Application through better alignment to business workflows and report functionality.

The Application has not been appropriately aligned to all clinical workflows. This has resulted in the use of manual workarounds and in some instances the need for new workarounds and repetitive manual entry of patient information. This is inefficient and increases the likelihood of errors.

We were advised by staff of manual workarounds to compensate for system instability. Activities being manually tracked in spreadsheets rather than using the reporting module include clinical coding for medical rebates and the correction of medical record entry errors.

The Application does provide the reporting functionality to track these activities, however staff reported that the system becomes unresponsive and unstable when running reports. In addition, we were not able to obtain information on the number of records manually scanned into the Application each month, to understand the use of the system, due to staff concerns that running reports would cause the system to crash.

Weak information security controls place sensitive records at risk of inappropriate access and misuse

We identified gaps in the controls to secure confidential patient records. These included:

- **Inadequate vulnerability management** – The DoH does not have an effective process in place to identify, assess and address known software vulnerabilities in a timely manner. These vulnerabilities could be used to gain unauthorised access to sensitive data or disrupt systems. We conducted vulnerability scans on key Application servers and identified 54 critical and 102 high severity vulnerabilities as a result of software updates that had not been applied.

- **Weak password configuration** – Analysis of the network accounts identified that around 40% have weak passwords, including a high number of privileged accounts. Access to the Application requires an enabled Application account and access to the WA Health network. Weak password configuration makes the system susceptible to password guessing attacks. This could lead to unauthorised access to patient information and further exploitation of DoH systems.

- **Ineffective user account management** – There is no process to routinely review who has access to the Application and to monitor user activity.

  Analysis of Application accounts identified approximately 5,500 accounts (15%) that have not logged on to the system for over 12 months. Without appropriate user account management controls, there is an increased risk of unauthorised or inappropriate access to patient information.

- **Insufficient continuity management processes** – Health Support Services has not developed appropriate business continuity or disaster recovery management processes. In addition, the maximum acceptable unavailability times and priority for the Application to be restored in the event of an incident has not been defined. Without an up to date and tested Business Continuity Plan (BCP) and Disaster Recovery Plans (DRP) there is an increased risk that key business functions and processes will not be restored in a timely manner after a disruption.

- **Application risks are not being formally managed –** There is no framework in place that outlines how the Application's risks are to be identified, assessed, managed and escalated on a routine basis. In addition, there is no mechanism to ensure the Application's risks are appropriately considered in the risk frameworks across the Health system. Without an effective risk management process, applications, may fail to meet business needs.

  While an Application risk analysis was conducted during the commissioning of Fiona Stanley Hospital, it has not been reviewed since. In addition, there were multiple 'High' application risks that were still present when the system went live.

- **Out of date design documentation** – Documentation created as part of the Fiona Stanley Hospital commissioning in 2014 has not been updated and does not capture alterations in the system design or new interfaces to other systems (internal and external to WA Health). Without a clear understanding of system interfaces and functionality, there is an increased risk of system failure in the event of changes, incidents or a disaster recovery event. Further, there is a risk of inappropriate access to information by exploiting weaknesses in the interfacing systems.

Recommendations

The DoH should:

1. embed appropriate contract management practices
2. develop appropriate processes to support future decisions to deploy applications, including approving business cases which are supported by appropriate cost models
3. review its information security policies to apply appropriate controls to protect sensitive information. Embed the policy across WA Health.

   - **DoH response:** Agreed
   - **Implementation timeframe:** by 31 December 2018

4. develop, approve and communicate a digital strategy to guide WA Health's approach to digitising medical records

   - **DoH response:** Agreed
   - **Implementation timeframe:** by 30 June 2019

5. conduct analysis to determine the business needs and assess if the Application is capable of meeting those needs
6. clearly communicate the roles and responsibilities for the management of the Application, including who has the authority to analyse, prioritise and approve operational activity.

   - **DoH response:** Agreed
   - **Implementation timeframe:** by 31 December 2019.

Response from Department of Health

The Department of Health (DOH) welcomes the application control and management review by the Auditor General as a means of identifying areas for improvement across the system. The benefits of a digital medical record for the WA health system cannot be underestimated and its implementation across several health sites has shown its value in providing quality and timely patient care.

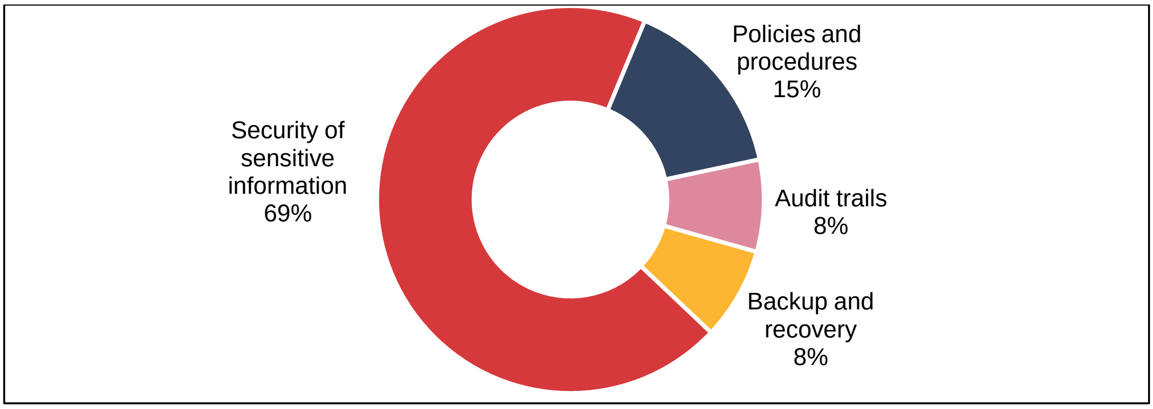
The DOH is in the process of developing a Digital Health Strategy to guide the appropriate investment and implementation of core systems including digital medical records.

Contract management processes for applications will be subject to continuous improvement reviews to ensure all costs are identified, tracked and managed.

The DOH notes that Health Service Providers provide different clinical services and is committed to working with clinicians to improve the use of applications in clinical workflows. This may require variation in application use between sites where applicable.

The DOH acknowledges the weak information security controls that were identified and notes that a Digital Information Security Program is now in place to address the issues raised.

Tenancy Bonds Management System – Department of Mines, Industry Regulation and Safety



Introduction

The Tenancy Bonds Management System (TBMS) is used by the Department of Mines, Industry Regulation and Safety (DMIRS) to manage the processing of residential and long stay tenancy bonds. The system stores confidential information including individual's driver's licence and banking details.

Conclusion

The TBMS supports DMIRS to manage the lodgement, variation and disposal of tenancy bonds. However, DMIRS's current security controls are not effective in protecting the confidentiality, integrity and availability of the information it stores.

Confidential tenant information is at risk of exposure due to weak passwords, inadequate user management and poor database management practices. System integrity is also at risk due to missing software updates, insufficient event monitoring, lack of risk assessments, and out of date system support documentation.

Information sharing with third parties is not secure, which we first raised with DMIRS in 2016. This increases the risk of unauthorised access to confidential information and needs to be addressed.

Background

A security bond is an upfront payment made by a tenant to cover any outstanding costs at the end of a tenancy. The bond is held in trust by the Bond Administrator, which is DMIRS. To carry out this role, DMIRS uses the TBMS to maintain proper account and transaction records as required under the *Residential Tenancies Act 1987*.

Bonds can be lodged with DMIRS, by post, email or in person. DMIRS uses the TBMS to process bond forms and provide workflow, management and reporting functions. It is a custom-built application, developed and maintained by DMIRS.

The TBMS is used by registered real estate agents to transact bonds using the internet portal, BondsOnline. The Magistrates Court also use the system for court ordered bond disposals back to the tenant. In September 2016, it became mandatory for real estate agents to lodge bonds using BondsOnline.

Each month DMIRS processes an average of:

- 9,400 bond lodgements, of which around 83% are processed electronically by real estate agents
- 1,500 variations to bond agreements
- 8,500 disposals of bond money at the end of a tenancy, of which around 48% are processed electronically by real estate agents.

At the end of September 2017, DMIRS held $353.5 million worth of bonds in trust.

Audit findings

Inadequate access controls increase the risk of unauthorised access or misuse

We found weaknesses with access controls for TMBS. Ensuring users are appropriately authorised and authenticated is vital to the security of the personal information stored within the application. We identified:

- **Weak password configuration** – The password configuration for the BondsOnline portal is inadequate and does not meet good practice for minimum length, complexity, ageing and reuse. We found that 10% of the BondsOnline passwords were very weak and there was no account lockout policy. Weak password configuration and a lack of lockout policy make the portal susceptible to password guessing attacks. This could lead to unauthorised access to the application data and allow further exploitation of DMIRS's IT systems.
- **External user accounts are not well managed** – Real estate agents are responsible for managing their own BondsOnline user accounts but overall responsibility for user management lies with DMIRS. While DMIRS manages internal access to the application well, the same controls are not applied to external access by third parties. Around 23% of external BondsOnline user accounts had not accessed the system in over a year. Dormant user accounts increase the likelihood of unauthorised or inappropriate access. For example, staff leaving a real estate agent could use a dormant account to access the application and information.
- **Insecure logins** – Information to access the application is not encrypted. This creates a vulnerability that could compromise DMIRS's other systems.

Security vulnerabilities are not well managed, leaving TBMS exposed to attacks

DMIRS does not effectively protect its systems from the threat of cyber-attacks. Software vulnerabilities can be exploited to gain unauthorised access to sensitive data or interrupt DMIRS's business. Regular patching and vulnerability scans are important for securing systems, however DMIRS:

- does not have a vulnerability management policy
- has not endorsed, and is not following, its patch management procedure
- is not using its vulnerability scanning software to perform regular scans to identify vulnerabilities in its IT environment to ensure patches are effective.

Our vulnerability scans of the key TBMS servers identified 975 vulnerabilities. Of these:

- 182 were rated critical and 793 rated high
- 508 had publicly available exploits on the internet that can be used by hackers to access the servers.

We also found that the server which grants user access to the BondsOnline portal is unsupported by the vendor. The system no longer receives security updates to protect the confidentiality and availability of the system.

The TBMS was last updated in November 2016, in addition, there were a number of patches released by the vendor since January 2015 that have not been applied. These include patches which address known security vulnerabilities. Timely application of patches is important for protecting the database.

Our external vulnerability assessment identified a number of default settings and misconfigurations that weaken the security of the system. These included:

- the use of a legacy security protocol that has known vulnerabilities
- the use of encryption algorithms that are weak and known to have been compromised
- default application settings that make it susceptible to cyber-attacks.

Sensitive data is at risk of exposure due to insufficient security controls

The TBMS stores personally identifiable information of tenants and owners, much of which is confidential. DMIRS' current security controls are not effective in protecting the confidentiality, integrity and availability of the information it stores. Some of the weaknesses we noted were:

- **Sharing data with third parties** – DMIRS shares personal information from the TBMS with a third party using an insecure file sharing portal. The portal does not require a username or password to download information, which is sent in clear text and not secured using encryption. Sharing sensitive information with third parties without adequate controls increases the risk of data theft.

  This weakness was first highlighted to DMIRS in our June 2016, Information Systems Audit Report.

- **Insecure access to documents** – DMIRS stores documents relating to bonds in its recordkeeping system. These include bond lodgement, variation and disposal documents as well as other communication with tenants and agents. Sensitive information from 100-point identity checks, such as a driver's licence information, is also stored in the system. Our review of the recordkeeping system identified accounts with inappropriate access to these sensitive documents. Appropriately managing who has access to bond documents within the recordkeeping system is important to reduce the risk of unauthorised access to, or modification of, these documents.

- **Sensitive information is not de-identified** – Sensitive information including bank account details are not encrypted within the TBMS database. In addition, DMIRS uses personal information in its development and testing databases, which do not have the same security controls. This data is not de-identified, which if inappropriately accessed, increases the risk of sensitive personal information being misused.

- **Database passwords were easily guessed** – We identified 36 accounts with easy to guess passwords for the network systems and the TBMS application. Twenty-one of these are inactive system accounts which have not had their default passwords changed. Four accounts were highly privileged accounts which are often targeted by malicious attacks. Easy to guess passwords are inconsistent with good practices and increase the likelihood of unauthorised access.

Inadequate monitoring means unauthorised access or changes may go undetected

DMIRS does not have a formal policy or procedures in place for the logging and monitoring of key activities in the TBMS. The server which grants user access to the BondsOnline portal is not monitored, and unsuccessful login attempts to the portal are not recorded. Although the TBMS application and supporting infrastructure record many events, these are only reviewed on an ad hoc basis.

Analysis of successful login attempts may provide insight into unauthorised activity such as inappropriate access to information and changes to records. Monitoring failed login attempts could reveal an attempt to break into the system. Without appropriate logging and monitoring policy and procedures DMIRS may not be able to detect unauthorised access or malicious activity.

Information technology risks to the TBMS have not been assessed

DMIRS has not assessed information technology risks to the TBMS application and information. Good risk management enables DMIRS to identify, assess and treat risks in a structured fashion. It also ensures decisions around risk are considered and actioned by suitable levels of governance. Without a risk assessment, senior management are less likely to know if implemented controls are managing the risks to the application within DMIRS's risk appetite.

In addition, DMIRS has not updated its IT risk register for over a year. An out of date risk register may not represent the current threat and control environment. As a result, DMIRS may not be adequately managing existing and new risks to the application.

DMIRS manages sensitive information and a breach of this may have serious implications for the individuals involved and may also cause reputational damage to DMIRS. To ensure that DMIRS is protecting this information it is essential that risks to the application are regularly considered and controls to mitigate are in place.

Backup testing and updated documentation is required to ensure ongoing and effective support for the TBMS

The TBMS application and information is backed up on a regular basis, but DMIRS does not regularly test these backups. Testing of backups is important to ensure that all the information required to recover the application is being backed up and restoration procedures work as expected.

We also found that while DMIRS has good procedures in place to manage continual enhancements to the TBMS, it does not have updated system support documentation. The documentation contained references to functions that were no longer in use and needs to be updated to reflect changes since the original release of the application.

Up to date documentation is required to effectively support the application and ensure that key application knowledge is not lost. This is particularly important to DMIRS as fixes and enhancements to the application are made by a contractor.

Recommendations

DMIRS should:

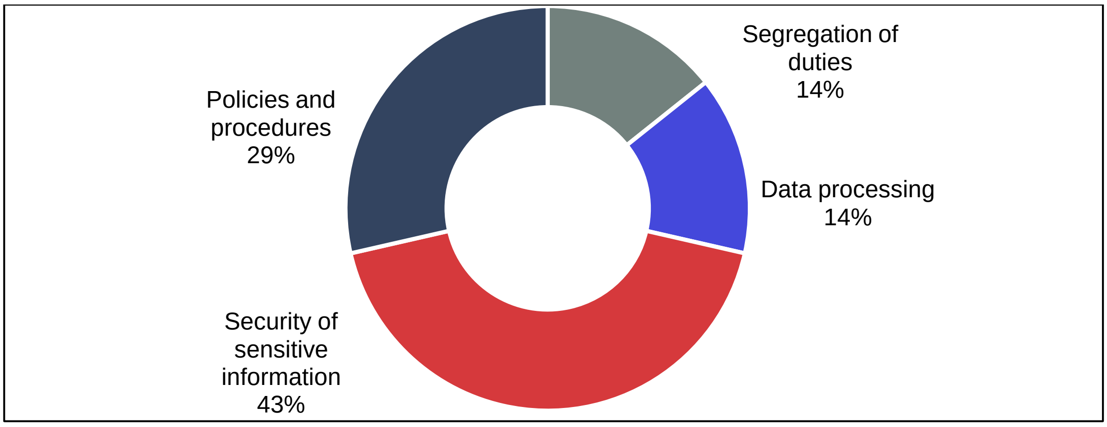
1. review and improve user access controls:
   a. so that application passwords comply with relevant better practice
   b. to periodically review external user accounts and determine if they are still required
   c. to secure access to the application
      - **DMIRS response:** Agreed
      - **Implementation timeframe:**
        a. resolved
        b. by September 2018
        c. resolved
2. review and enhance the process for managing security vulnerabilities and software updates
   - **DMIRS response:** Agreed
   - **Implementation timeframe:** by March 2019
3. implement appropriate controls to protect sensitive information, which may include encryption
   - **DMIRS response:** Agreed
   - **Implementation timeframe:** by December 2018
4. develop and implement logging and monitoring policies and procedures
   - **DMIRS response:** Agreed
   - **Implementation timeframe:** by December 2019
5. conduct an ICT risk assessment for the TBMS application and update the information services risk register
   - **DMIRS response:** Agreed
   - **Implementation timeframe:** by November 2018
6. establish and implement a procedure to routinely test restoration of backups
   - **DMIRS response:** Agreed
   - **Implementation timeframe:** by December 2018
7. review and update application support documentation
   - **DMIRS response:** Agreed
   - **Implementation timeframe:** by November 2018.

Response from the Department of Mines, Industry Regulation and Safety

Thank you for the opportunity to respond to the Tenancy Bonds Management System audit findings.

The Department of Mines, Industry Regulation and Safety accepts the findings and agree with all recommendations. DMIRS has reviewed its Cyber and Information Management Framework (CISM) and is implementing it across all of DMIRS systems, including the Tenancy Bonds Management System. The CISM covers all aspects of security including password complexity standards and routine audits of business system accounts.

First Home Owner Grant Online – Office of State Revenue



Introduction

The First Home Owner Grant Online system (FHOG Online) is used by the Office of State Revenue (OSR) to provide a one-off payment for eligible first home owners who are buying or building a new home. The system contains confidential personal information about grant applicants, including bank account details.

Conclusion

The FHOG Online system stores and processes grant applications and payments as required. While we did not find any instances of inappropriate access or misuse, confidential information, including applicant bank details, is at risk of exposure due to inadequate information security and informal change management procedures. There are also extensive manual processes which has made OSR's use of the system inefficient and increases the risk of errors.

Background

The OSR is a business unit of the Department of Finance. It administers revenue laws and grant and subsidy schemes, including the FHOG.

The FHOG assists eligible first home owners to buy or build a residential property as their principal place of residence. The grant process is a shared responsibility between the OSR and the Department of Treasury. OSR receives applications and assesses eligibility for grants. Treasury is responsible for paying the money to eligible grant applicants.

FHOG applications can be submitted through approved agents or directly with the OSR. Applications are recorded and managed in the FHOG Online system. The system was developed and is maintained by a third party vendor.

In 2016-17, almost 15,630 grant applications were recorded and managed in FHOG Online.

Audit findings

Confidential information is at risk of unauthorised access due to insufficient security controls

FHOG Online stores personal and sensitive information of applicants, much of which is confidential such as bank account details of grant recipients. The OSR's security controls are not effective in protecting the confidentiality, integrity and availability of the information it stores. Weaknesses we found include:

- **Unprotected personal data in test environment** – We found that confidential information is used and retained in the test environment even though the test environment does not have the same level of security. Processing and storing this information in the test environment without appropriate levels of protection increases the risk that it may be misused or compromised.
- **Passwords were easily guessed** – We identified database user accounts, including highly privileged database administrator accounts, with easy to guess passwords. Examples include passwords that are the same as usernames and passwords 3 characters in length. We also found that users are not forced to change passwords on the database server after a period of time. The passwords for all privileged accounts had not been changed in over 2 years.

No segregation of duties increases the risk of grants being issued inappropriately

The Department of Treasury has not segregated its grant payment processes. We found the same person in Treasury processes grants payments and performs payment reconciliations. This lack of segregation of duties increases the risk of inappropriate grant payments.

The files used during the payment process contain bank account details, which are stored in plain-text format. These payment files can be amended before uploading to the bank for payment and there is no independent process to detect changes made to the original files. Although an independent check is performed to verify the summary of payment amounts and total transactions, it does not validate bank account details.

Manual processes are inefficient and increase the risk of errors

The OSR relies on a substantial amount of manual processing to collate information in the system. Manual workflows are inefficient and increase the risk of errors in determining the applicants' eligibility.

Examples of manual processing include:

- Grants officers in OSR manually check external systems to verify that applicants satisfy a number of criteria including criteria around property ownership, citizenship and residency. These include systems at the WA Land Information Authority, Water Corporation, Western Power and the WA Electoral Commission. There is no electronic interface between the government databases.
- The FHOG system does not allow automated workflows to notify staff when applications require additional investigation. Instead, a manual spreadsheet is used to record tasks when grant officers cannot determine the eligibility of the applicant.

Automated workflows and links or interfaces with other government agency databases can significantly improve the integrity and efficiency of processing applications.

Poor IT controls make FHOG Online more vulnerable to unauthorised access

The FHOG Online system is vulnerable to external threats and inappropriate access. To ensure the system continues to be reliable and information secure, the OSR needs to improve its IT controls.

Some of the gaps we identified were:

- **Lack of regular vulnerability assessments –** The OSR does not have an effective process in place to identify, assess and address known software vulnerabilities in a timely manner. We conducted scans on key FHOG Online servers and identified critical and high severity vulnerabilities due to missing third party software updates (patches). We were able to exploit these vulnerabilities to access confidential information and escalate our privileges for further access.
- **No process to manage changes to the system** – The OSR sends ad hoc requests to a service provider to resolve system issues and make changes to the FHOG Online system. However, it does not have change management procedures in place to formally document, review and approve change requests. There is a risk that management will not know of these changes or appropriately manage associated risks.
- **User permissions are not reviewed –** The OSR does not regularly review privileges and access to the FHOG Online system. We found that the system cannot produce a report to assist with verifying whether the roles of its users are appropriate. Without review of user access, there is an increased risk of unauthorised or inappropriate access going undetected. The OSR has an appropriate Monitoring Systems Use Policy that requires regular internal audits on all aspects of user access and use of the FHOG system. However, the policy is not followed.

Recommendations

The OSR should:

1. review its information security policy to apply:
    a. appropriate controls to protect sensitive information
    b. system account passwords that comply with relevant industry good practice guidelines
        - **OSR response:** Agreed
        - **Implementation timeframe:** Completed
2. review manual processes and if appropriate, automate them
    - **OSR response:** Agreed
    - **Implementation timeframe:** June 2020
3. review the vulnerability management process, conduct regular vulnerability assessments and apply software updates recommended by vendors
    - **OSR response:** Agreed
    - **Implementation timeframe:** Completed
4. define and follow a change management process
    - **OSR response:** Agreed
    - **Implementation timeframe:** Completed
5. implement procedures and controls for user access management in line with the existing internal policy.
    - **OSR response:** Agreed
    - **Implementation timeframe:** Completed

The Department of Treasury should:

1. address the risks associated with the segregation of duties in relation to the payment and reconciliation processes
    - **Department of Treasury response:** Agreed
    - **Implementation timeframe:** Completed.

Response from the Office of State Revenue

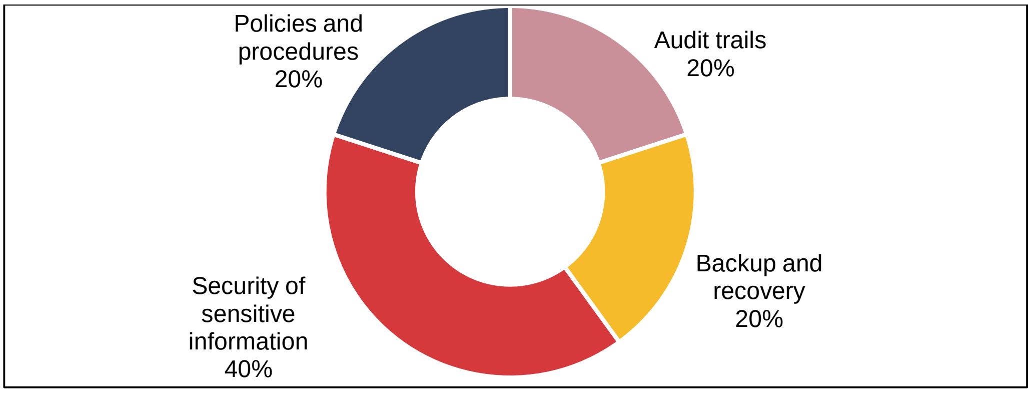
The Department of Finance, Office of State Revenue has agreed to all of the recommendations set down in the draft management letter received in November 2017 and the subsequent management letter received in February 2018.

The Department of Treasury has also agreed with the recommendation it was responsible for. Both Departments accept the findings will strengthen the operation of the FHOG system and its supporting operations and will mitigate risks within the current processes.

Since receiving the draft management letter, the Department of Finance and Department of Treasury implemented changes to address the risks that were identified in respect of all findings in the audit.

The finding to automate the manual processing of pre-compliance data checking on first home owner grant applications has been addressed and will be actioned on a best endeavours basis. To automate data checking requires system enhancements and which will be prioritised alongside future planned system upgrades to State Revenue's systems.

Election Management System WA – Western Australian Electoral Commission



Introduction

The Election Management System WA (EMSWA) is used by the Western Australian Electoral Commission (WAEC) to manage election related information. This includes EMSWA storing an electronic electoral roll, and recording and counting votes for State general elections. The system stores voter personal information such as name, address, telephone numbers and date of birth.

Conclusion

The EMSWA system essentially achieves its purpose. However, we found a number of issues that may compromise the security and integrity of sensitive data, including voter identity details.

While we did not find any instances of inappropriate access or misuse, confidential information is at risk due to insufficient password controls, unencrypted databases and minimal tracking or monitoring of changes made to the data. The availability of the system is also at risk due to a lack of documented and tested disaster recovery plan.

Inefficient manual transfer of data from other related sources into the EMSWA system may compromise the integrity of the information in the EMSWA system.

Background

The WAEC aims to provide all Western Australians with accessible, efficient and high quality electoral and enrolment services.

It is responsible for maintaining the State's electoral roll and conducting parliamentary elections and referenda, local government elections and other statutory and non-statutory elections. WAEC also promotes community awareness of the electoral process.

In the State general election on 11 March 2017, there were 1,593,222 people enrolled to vote and 1,411,829 votes counted.

Completed ballot paper information was recorded and processed through EMSWA, which is developed and maintained by WAEC.

Audit findings

Security weaknesses increase the risk of inappropriate access and misuse of voter personal information

The EMSWA system stores confidential personal information about voters such as name, address, telephone numbers and date of birth. If accessed inappropriately this information could be used for identity theft. While we found no instances of this information being inappropriately accessed or misused, we did identify security weaknesses, including:

- **Insecure databases –** The password policy is not enforced for database user accounts and the password for the System Administrator account had not been changed for over 2 years. Administrator and database accounts are the first accounts an attacker will try to compromise in order to gain unauthorised access to systems. We also found that data encryption is not used to protect sensitive information in the EMSWA databases, leaving this information more vulnerable to misuse if inappropriately accessed.
- **Unprotected personal information** – We found that confidential personal information of voters from the EMSWA live system is copied and used in the test environment which does not have the same level of security. Processing and storing this information in test systems without appropriate levels of security increases the risk that it may be compromised.

WAEC does not have documented processes to recover the EMSWA following a major incident or disruption

WAEC does not have an IT Disaster Recovery Plan (DRP) that details the processes to recover its information systems following a major incident or disruption. This could compromise the continuity and integrity of election processes and the delivery of key services, and potentially damage the reputation of the WAEC.

While the WAEC has recovery procedures in place, these are not fully documented and tested.

An IT DRP is a key document that provides details of procedures to be followed to recover systems in the event of an incident or disruption. Without an appropriately tested IT DRP it is not possible to confirm the effectiveness of the plan and the ability of the WAEC staff to execute it.

WAEC does not know whether inappropriate or unauthorised changes are made to the EMSWA information

The WAEC does not have a formal policy or procedure in place to manage the logging and monitoring of key events. The EMSWA does not capture user logon activities or who made changes to electoral roll information. Without effective system logging and proactive monitoring of these logs the WAEC cannot identify and act on any suspicious events or user activities.

Manual processes are inefficient and increase the risk of errors in the EMSWA

Information from a number of internal systems is manually entered into the EMSWA, increasing the likelihood of errors.

Examples of manual processing that could be automated to increase efficiency and reduce the risk of errors include:

- Legislative Council ballot paper information is manually entered into an application called CountWA. After results are calculated in this system, a subset of the results are then manually entered into the EMSWA system.
- Legislative Assembly ballot paper information is manually entered into spreadsheets. This information is then manually imported into the EMSWA system.

These processes could be automated within the EMSWA to draw the information directly from CountWA and spreadsheets.

Recommendations

The WAEC should:

1. enforce its password policy for all users including administrator accounts
2. review the risks associated with storing confidential personal information and assess options to protect it from unauthorised access and misuse
3. a. develop, regularly review and test the IT DRP

   b. develop and implement an effective framework for monitoring and logging of key change events

   c. implement appropriate information security controls to protect sensitive information in the test environment
4. a. review election systems to identify key events or transactions that require logging and monitoring

   b. review manual data transfer processes and consider if they can be automated
5. complete, test and implement changes to election systems in readiness for the State General Election in March 2021.

Response from the Western Australian Electoral Commission

The Western Australian Electoral Commission welcomed the application controls review of the Election Management System WA (EMSWA) and provides the following acceptance of the recommendations from this review.

Recommendation 1: Accept fully

Password complexity policies will be enforced on all SQL accounts. Password expiration policies will be enforced on all SQL accounts where appropriate. Application specific accounts will be controlled via a manually scheduled password change regime to ensure election system uptime. This is currently being implemented and is targeted for completion by 31 August 2018.

Recommendation 2: Accept fully

A review of the risks associated with storing confidential information and options to protect it will be conducted in conjunction with our Risk Management and Audit Committee by 30 September 2018.

Recommendation 3: Accept fully

Development of the IT DRP reflecting the Commission's current DR solution will commence shortly and be completed and tested by 31 December 2018 with an annual review and test being scheduled.

A framework to capture key change event audit logs will be developed by 31 December 2018 with implementation scheduled with election system changes due to be completed by 30 June 2020.

Safeguards to mask and protect sensitive information used in the test environments will be implemented by 31 December 2018.

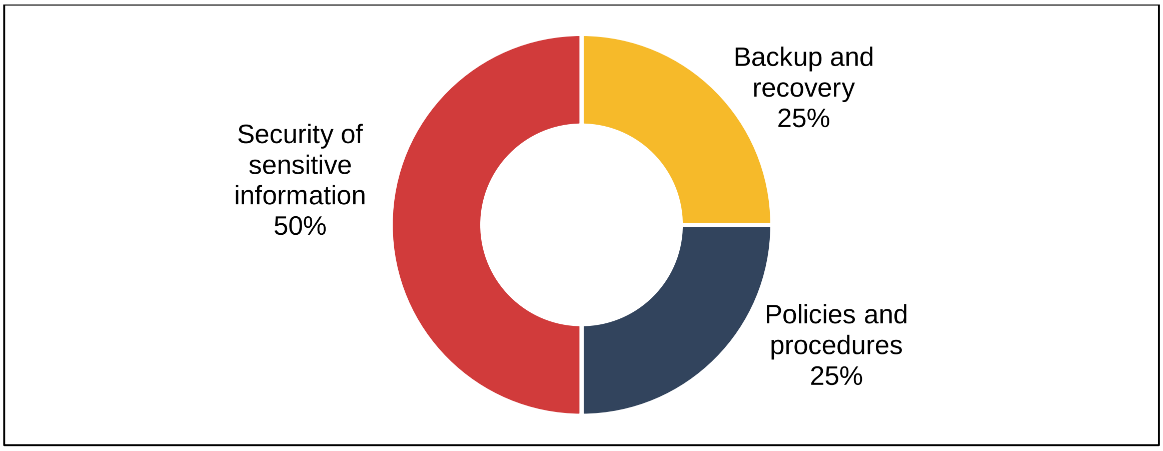
Recommendation 4: Accept fully

A review to identify key events or transactions that require logging and monitoring and manual data transfer processes that can be cost effectively automated will be conducted in conjunction with our Election Management Committee by 30 June 2019.

Recommendation 5: Accept fully

Changes to election systems will be completed, tested and implemented by 30 June 2020, well in advance of the next State General Election in March 2021.

Keysmart – Keystart Housing Scheme Trust



Introduction

Keystart Housing Scheme Trust uses the Keysmart system to manage home loan enquiries, application processing, broker commissions and loans. The system stores confidential information including loan applicants' proof of identity, bank account details, marriage status and proof of employment.

Audit Conclusion

Keysmart achieves its purpose, enabling Keystart Housing Scheme Trust to manage the operations of its business. However, to better protect customers' personal and credit information, Keystart needs to enhance the security of the system. This includes better user access management, stronger passwords and regular software updates.

Background

Keystart was established in 1989 by the Western Australian government to provide secured and low-deposit home loans to Western Australians. Keystart assesses, approves, manages and discharges its home loans using the Keysmart application.

Applicants can submit their loan applications to Keystart in person at an office location or online. They can also use a broker, who can enter the loan on the applicants' behalf using the Keysmart broker portal.

Loan applications include personal information such as proof of identity, financial statements, marriage status and proof of employment. Once the loan is finalised Keystart uses Keysmart to manage the life of the loan and pay broker commissions. Approved applicants can also view their loan activity through the Keysmart client portal.

The Keysmart application was developed in-house. In 2017, it was used to process an average of 306 applications and approve about $62.6 million worth of loans each month.

Audit findings

Inadequate user management and weak passwords increase the risk of unauthorised access to loan information

Keysmart holds confidential information on loan applications and approvals and good user access management is critical for its protection. Keystart has a user access management policy describing the creation, change, removal and review of user accounts. However, we found the policy to be inadequate as it does not apply to privileged, system and database accounts. Further, the user account review process does not state when and how the reviews will be undertaken, and by whom.

We also identified:

- **Unused system accounts** – 32 system accounts that had not been used for 1 to 8 years. These accounts increase the opportunities available to an attacker to gain access to information.
- **Weak database passwords** – 20 accounts with easy to guess passwords. Fifteen of these were default passwords for disabled system accounts. These accounts generally have higher privileges and their default passwords are well known. It is good practise to change the default password for these accounts even though they are disabled. In addition, we found 11 accounts that have not had their passwords changed for over 6 years. Without appropriate database security there is an increased risk of unauthorised access to information.

Vulnerabilities exist due to inadequate configuration of software updates

Keystart has a vulnerability management process in place, however we identified vulnerabilities on a number of servers and workstations, including the Keysmart application and its underlying database.

We identified 4 critical and 53 high rated vulnerabilities which may be exploited to gain access to systems and disrupt business operations. This was mainly due to inadequate configuration of applied patches making them ineffective. Without effective vulnerability management there is an increased risk to the confidentiality, integrity and availability of Keystart systems.

Vulnerability assessments are important for the security of systems and should include proper configuration of patches as recommended by the vendor.

Recommendations

Keystart should:

1. identify and appropriately disable or remove any system accounts that are no longer required
2. review and enhance its access management procedures to include user, privileged, service and database accounts
3. review and enhance its technical vulnerability management process to apply software updates in a timely manner and in accordance with vendors' recommendations.

Response from Keystart Housing Scheme Trust

Keystart appreciates the importance of having adequate controls in place for corporate applications to protect information assets in the course of operational activities. As such we take the findings seriously and accept that there are some controls that need to be improved.

Keystart fully accepts:

Recommendation (1): Keystart has amended policy and procedure to include system accounts as part of its regular user audit, and has completed an audit under new policy.

Keystart accepts in part:

Recommendation (2): User access management procedures are already in place to review user and privileged accounts. As with recommendation (1), the policy and procedure has now been amended to include service and database accounts.

Recommendation (3): Keystart's compensating controls would minimise the impact of exploited vulnerabilities, in addition Keystart already applies software updates in a timely manner, however, acknowledges that some secondary actions to enforce those updates were not actioned – this has been addressed and corrected.

General computer controls and capability assessments

Introduction

The objective of our general computer controls (GCC) audits is to determine whether computer controls effectively support the confidentiality, integrity, and availability of information systems. General computer controls include controls over the information technology (IT) environment, computer operations, access to programs and data, program development and program changes. In 2017 we focused on the following control categories:

- information security
- business continuity
- management of IT risks
- IT operations
- change control
- physical security.

Conclusion

We reported 539 general computer controls issues to the 47 agencies audited in 2017 compared with 441 issues at 46 agencies in 2016. This increase is, in part, due to a more detailed assessment into all general control categories in 2017.

There was an increase in the number of agencies assessed as having mature general computer control environments across all 6 categories of our assessment. Ten agencies met our expectations for managing their computer environments effectively, compared with only 6 in 2016.

While system change controls and physical security are managed effectively by most agencies, 2 of the categories, information security and business continuity, have shown little improvement in the last 10 years. The majority of issues we have identified can be easily addressed with better password management and ensuring processes to recover data and operations in the event of an incident are kept updated.

By not prioritising the security and continuity of information systems, agencies risk disruption to the delivery of vital services to the community and compromise the confidentiality and integrity of the information they hold.

Background

We use the results of our GCC work to inform our capability assessments of agencies. Capability maturity models are a way of assessing how well developed and capable the established IT controls are. The models provide a benchmark for agency performance and a means for comparing results from year to year.

The models we developed use accepted industry good practice as the basis for assessment. Our assessment of the appropriate maturity level for an agency’s general computer controls is influenced by various factors. These include: the business objectives of the agency; the level of dependence on IT; the technological sophistication of their computer systems; and the value of information managed by the agency.

Audit focus and scope

We conducted GCC audits at 47 agencies. This is the tenth year we have assessed agencies against globally recognised good practice.

We provided 40 of the 47 agencies with capability assessment documentation and asked them to complete and return the forms at the end of the audit. We then met with each of the agencies to compare their assessment and ours, which was based on the results of our GCC audits. Seven agencies, whose GCC audits were outsourced, were not included in the capability assessment.

We use a 0-5 scale rating[5] to evaluate each agency's capability maturity level in each of the GCC audit focus areas. The models provide a baseline for comparing results for agencies from year to year. We have included specific case studies where information security weaknesses potentially compromise agencies' systems.

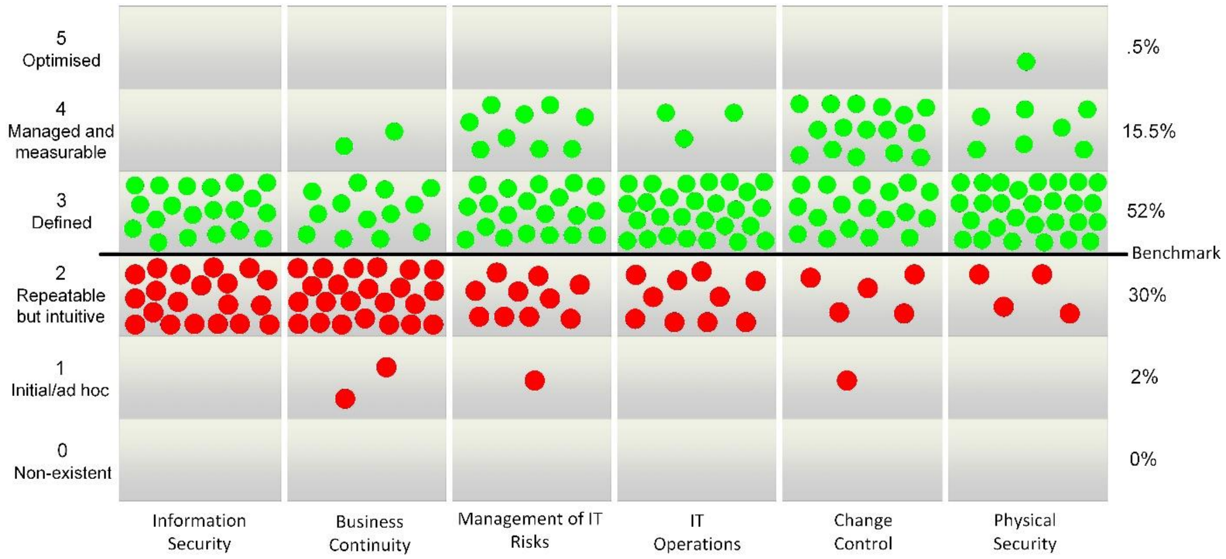
0 Non-existent	Management processes are not applied at all. Complete lack of any recognisable processes.
1 Initial/ad hoc	Processes are ad hoc and overall approach to management is disorganised.
2 Repeatable but intuitive	Processes follow a regular pattern where similar procedures are followed by different people with no formal training or standard procedures. Responsibility is left to the individual and errors are highly likely.
3 Defined	Processes are documented and communicated. Procedures are standardised, documented and communicated through training. Processes are mandated, however it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.
4 Managed and measurable	Management monitors and measures compliance with procedures and takes action where appropriate. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.
5 Optimised	Good practices are followed and automated. Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the agency quick to adapt.

Table 1: Rating criteria

Audit findings

Our capability maturity model assessments show that agencies need to establish better controls to manage information security, business continuity, IT risks and IT operations. Figure 1 summarises the results of the capability assessments across all categories for the 40 agencies assessed. We expect agencies to rate a level 3 (Defined) or better across all the categories.

[5] The information within this maturity model assessment is based on the criteria defined within the Control Objectives for Information and related Technology (COBIT) manual.



Source: OAG

Figure 1: Capability maturity model assessment results

The model shows that the categories with the greatest weakness were management of IT risks, information security and business continuity.

The percentage of agencies reaching level 3 or above for individual categories was as follows:

Category	2017 %		2016 %
Information security	50	↑	39
Business continuity	37	↑	27
Management of IT risks	72	↑	63
IT operations	75	↓	76
Change control	84	↑	78
Physical security	90	↑	85

Source: OAG

Table 2: Percentage of agencies at level 3 or above

The results for information security and business continuity show improvement, however, it is still of concern that only half or less of agencies were adequately controlled in these areas.

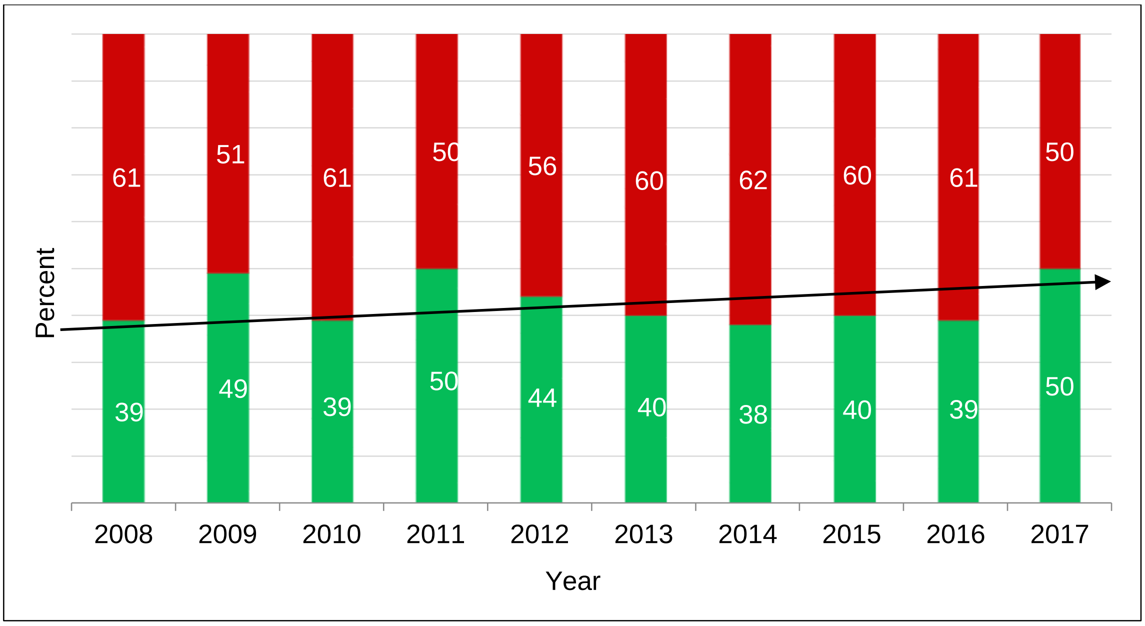
Of the agencies we review every year there are only 2 that have consistently demonstrated good management practices across all areas assessed:

- Department of the Premier and Cabinet (5 years at level 3 or higher)
- Racing and Wagering Western Australia (4 years at level 3 or higher).

Information security

Only 50% of agencies met our benchmark for effectively managing information security in 2017. This result was last achieved in 2011 with results declining up to 2016. It is clear from the basic security weaknesses we identified that many agencies are lacking some important and fundamental security controls needed to protect systems and information. The trend across the last 10 years shows little change on average and we expect agencies to improve controls regarding information security.

We assessed whether agency controls were administered and configured to appropriately restrict access to programs, data, and other information resources.



Source: OAG

Figure 2: Information security

Note: Green represents the percentage of agencies that met the benchmark and red represents the agencies that did not meet the benchmark.

Weaknesses we found included:

- information security policies did not exist, were out of date or not approved
- easy to guess passwords for networks, applications and databases, e.g. Password, Password1, guest or no password at all
- applications and operating systems without critical updates applied
- lack of processes to identify security vulnerabilities within IT infrastructure
- no review of highly privileged application, database and network user accounts.

Information security is critical to maintaining data integrity and reliability of key financial and operational systems from accidental or deliberate threats and vulnerabilities.

Specific examples where security weaknesses compromised agency information

Many agencies remain vulnerable to attacks from the internet and are at risk of being compromised. In 2017-18 we performed vulnerability assessments and reported thousands of security vulnerabilities on a small sample of key systems at agencies. Security issues ranged from weak passwords to software updates not being applied, malware infections, unauthorised access and disclosure of sensitive and confidential information.

We also performed tests that demonstrated agencies failed to detect the loss of information through the internet and were unaware of the risks. The following case studies demonstrate the risks to agency information when information is not securely managed.

Website vulnerabilities

We performed a vulnerability test on a system which was publicly facing via the internet. We were able to gain access with administrator privileges to a significant amount of information including sensitive data in this environment without the agency knowing.

Figure 3: Website vulnerabilities provide access to agency systems

Weak passwords

At one agency we found that easy to guess and known passwords such as password1, abcd1234, welcome1 are used for 443 out of 787 network access accounts. This represents a total of 56% of the population with weak passwords. We also note two passwords (abcd1234 and password1) are used by 131 and 161 users respectively.

These accounts are also used to gain remote access to finance, payroll and other key systems.

Figure 4: User accounts have weak passwords

Default credentials were not changed

Our high-level security check on finance and payroll databases in one agency found that the highly privileged database administrator account ‘sa’ was enabled and had a weak/default password. The agency’s policy stated this account should be disabled. In addition, the network administrator account also had administrator privileges on these databases and there is no logging of activity at the database level to know what access and changes are occurring.

Without appropriate controls and security in place, there is an increased risk that the confidentiality, integrity and availability of information is compromised.

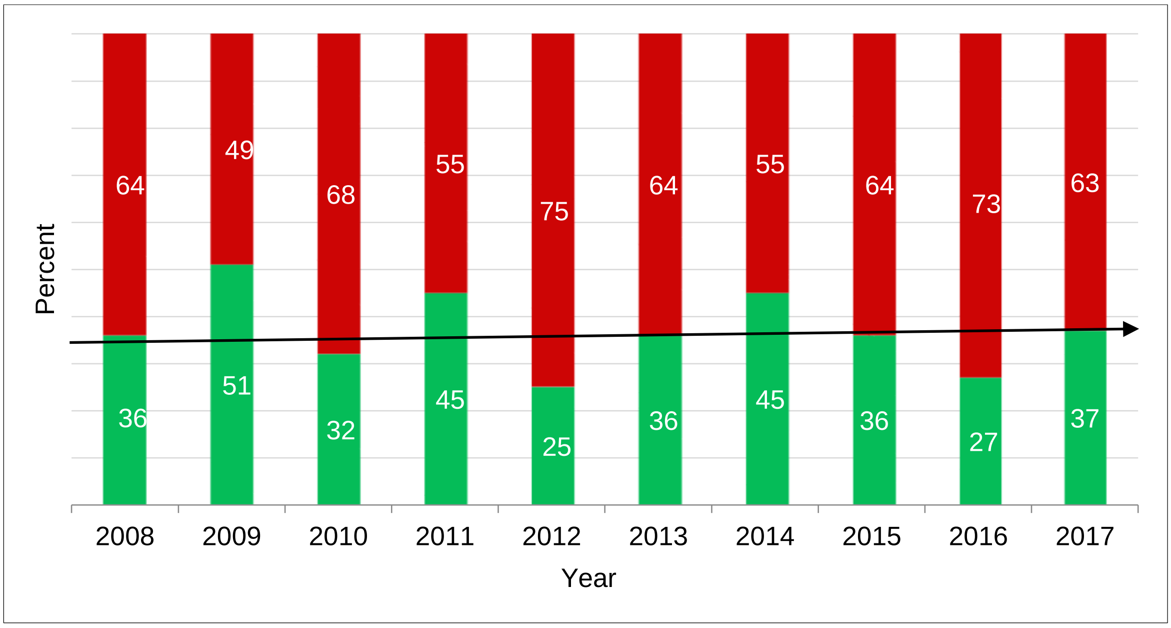
Figure 5: Default credentials could enable administrator level access

Business continuity

To ensure business continuity, agencies should have in place a business continuity plan (BCP), a disaster recovery plan (DRP) and an incident response plan (IRP). The BCP defines and prioritises business critical operations and therefore determines the resourcing and focus areas of the DRP. The IRP needs to consider potential incidents and detail the immediate steps to ensure timely, appropriate and effective response.

These plans should be tested on a periodic basis. Such planning and testing is vital for all agencies as it provides for the rapid recovery of computer systems in the event of an unplanned disruption affecting business operations and services. Senior executives should be monitoring that plans are developed and tested in accordance with the risk profile and appetite of the agency.

We examined whether plans have been developed and tested. Although we found a 10% improvement from last year, 63% of the agencies do not have adequate business continuity and disaster recovery arrangements in place. The trend over the last 10 years has shown agencies are not affording sufficient priority to disaster recovery and continuity.



Source: OAG

Figure 6: Business continuity

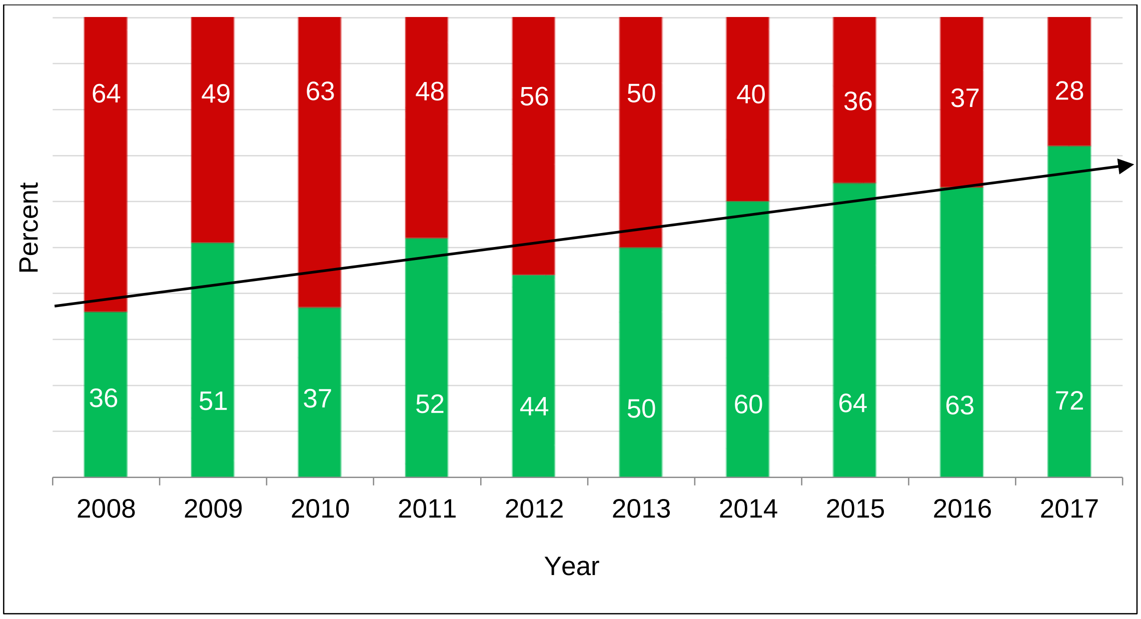
Weaknesses we found included:

- no business continuity or DRPs
- no incident management procedures
- tolerable outages for critical systems not defined
- old and redundant DRPs with some not reflecting current ICT infrastructure
- DRPs never tested and agencies do not know if they can recover systems
- backups never tested and not stored securely
- uninterrupted power supplies not tested or not functional.

Without appropriate continuity planning there is an increased risk that key business functions and processes will fail and not be restored in a timely manner after a disruption. Disaster recovery planning will help enable the effective and timely restoration of systems supporting agency operations and business functions.

Management of IT risks

Seventy-two percent of agencies met our expectations for managing IT risks, a 36% improvement since the first assessment in 2008, with agencies showing improved management controls over IT risks.



Source: OAG

Figure 7: Management of IT risks

Weaknesses we found included:

- no risk registers
- risk management policies in draft or not developed
- inadequate processes for identifying, assessing and treating IT and related risks
- risk registers not maintained, for ongoing monitoring and mitigation of identified risks.

All agencies are required to have risk management policies and practices that identify, assess and treat risks that affect key business objectives. IT is one of the key risk areas that should be addressed. We therefore expect agencies to have IT specific risk management policies and practices such as risk assessments, registers and treatment plans.

Without appropriate IT risk policies and practices, threats may not be identified and treated within reasonable timeframes, thereby increasing the likelihood that agency objectives will not be met.

IT operations

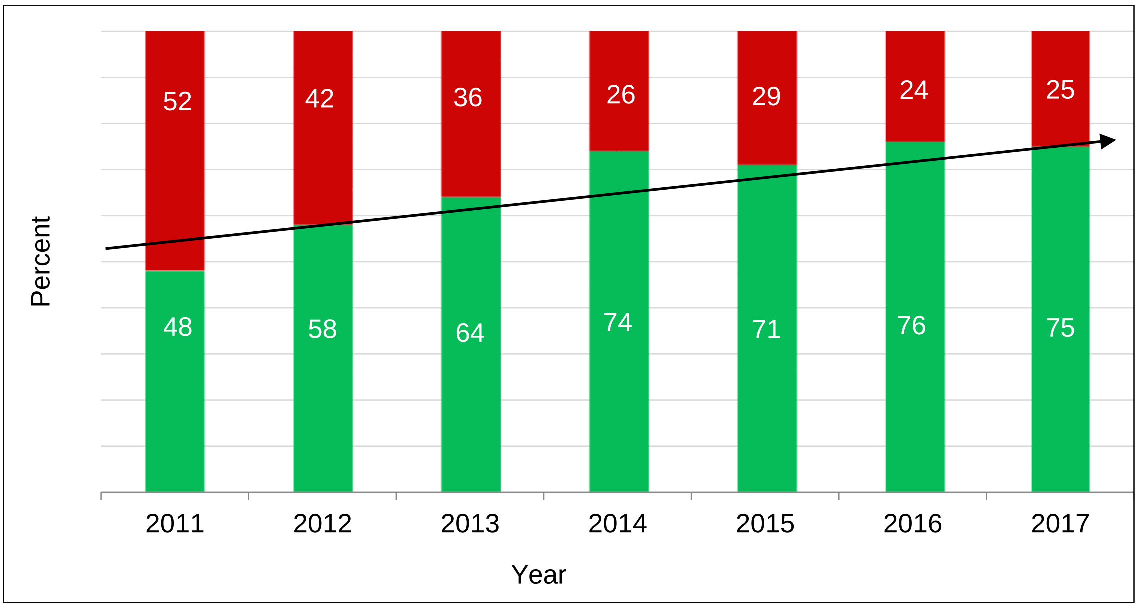
The rating for performance in IT practices and the service level performance provided to meet their agency's business decreased by 1% in 2017 to 75% compared to the previous year. However, there has been a steady improvement since 2011 when we first added this area to the CMM.

Effective management of IT operations is a key element for maintaining data integrity and ensuring that IT infrastructure can resist and recover from errors and failures.

We assessed whether agencies have adequately defined their requirements for IT service levels and allocated resources according to these requirements. We also tested whether service and support levels within agencies are adequate and meet good practice. Other tests included whether:

- policies and plans are implemented and working effectively
- repeatable functions are formally defined, standardised, documented and communicated

- effective preventative and monitoring controls and processes have been implemented to ensure data integrity and segregation of duties.



Source: OAG

Figure 8: IT operations

Note: data only available from 2011 when we added this area to the CMM.

Weaknesses we found included:

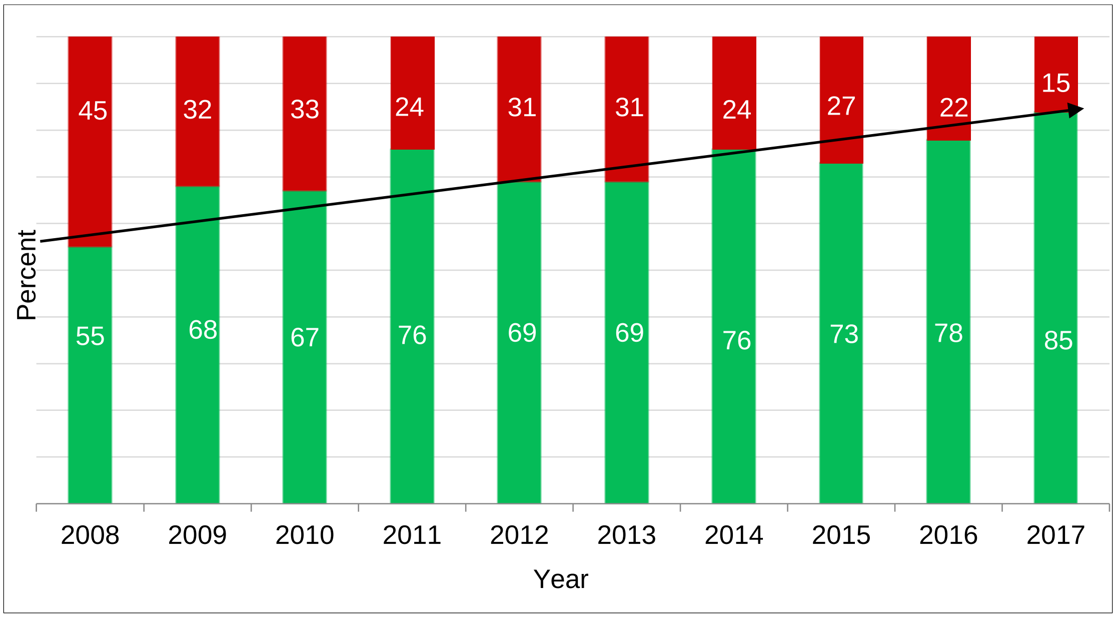
- information and communication technology strategies not in place
- lack of segregation of duties across finance, payroll and network systems
- no logging of user access and activity and no reviews of security logs for critical systems including remote access and changes to databases with confidential information
- former staff with access to agency networks and applications after termination
- unauthorised devices can connect to networks, such as USBs and portable hard drives
- lack of policies and procedures and weak governance over ICT operations
- several agencies are running unsupported operating systems
- asset registers not maintained and ICT equipment unable to be located.

These types of findings can mean that service levels from computer environments may not meet business requirements or expectations. Without appropriate ICT strategies and supporting procedures, ICT operations may not be able to respond to business needs and recover from errors or failures.

Change control

We examined whether system changes are appropriately authorised, implemented, recorded and tested. We reviewed any new applications acquired or developed to evaluate consistency with management's intentions. We also tested whether existing data converted to new systems was complete and accurate.

Change control practices have slowly been improving since 2008, with 34 out of the 40 agencies achieving a level 3 or higher rating.



Source: OAG

Figure 9: Change control

Weaknesses we observed included:

- no formal system change management policies in place
- changes to critical systems not logged or approved
- no documentation regarding changes made to systems and critical devices
- risk assessments for major changes to infrastructure not performed.

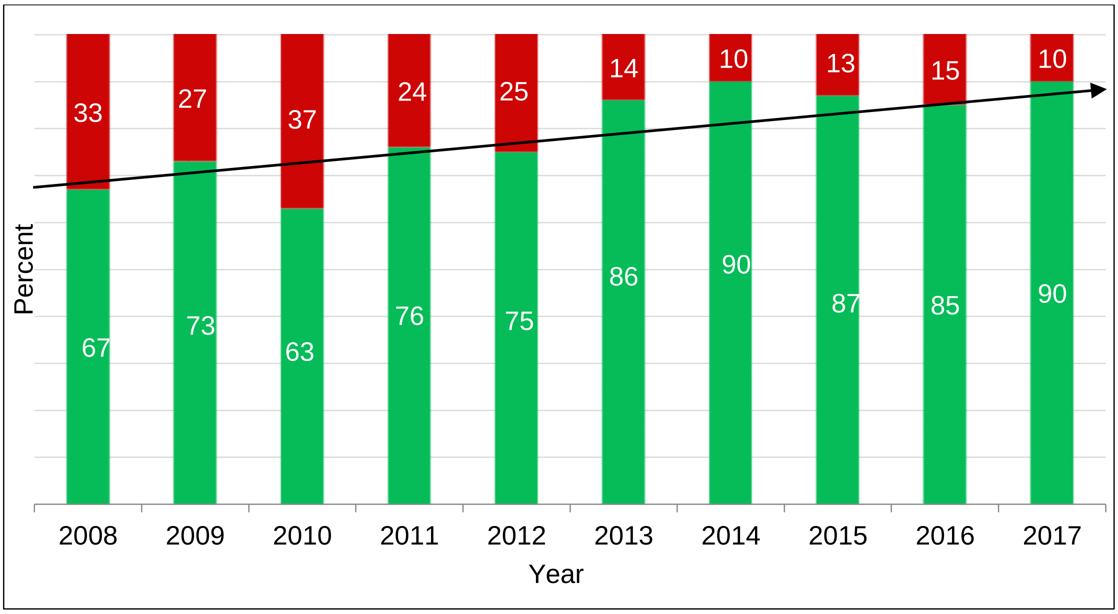
An overarching change control framework is essential to maintaining a uniform standard change control process and to achieving better performance, reduced time and staff impact and increased reliability of changes. When examining change control, we expect defined procedures are used consistently for changes to IT systems. The objective of change control is to facilitate appropriate handling of all changes.

There is a risk that without adequate change control procedures, systems will not process information as intended and agencies' operations and services will be disrupted. There is also a greater chance that information will be lost and access given to unauthorised persons.

Physical security

We examined whether computer systems were protected against environmental hazards and related damage. We also determined whether physical access restrictions are implemented and administered to ensure that only authorised individuals have the ability to access or use computer systems.

Thirty-six of the 40 agencies met our expectations for the management of physical security. This continues to be a generally well controlled area.



Source: OAG

Figure 10: Physical security

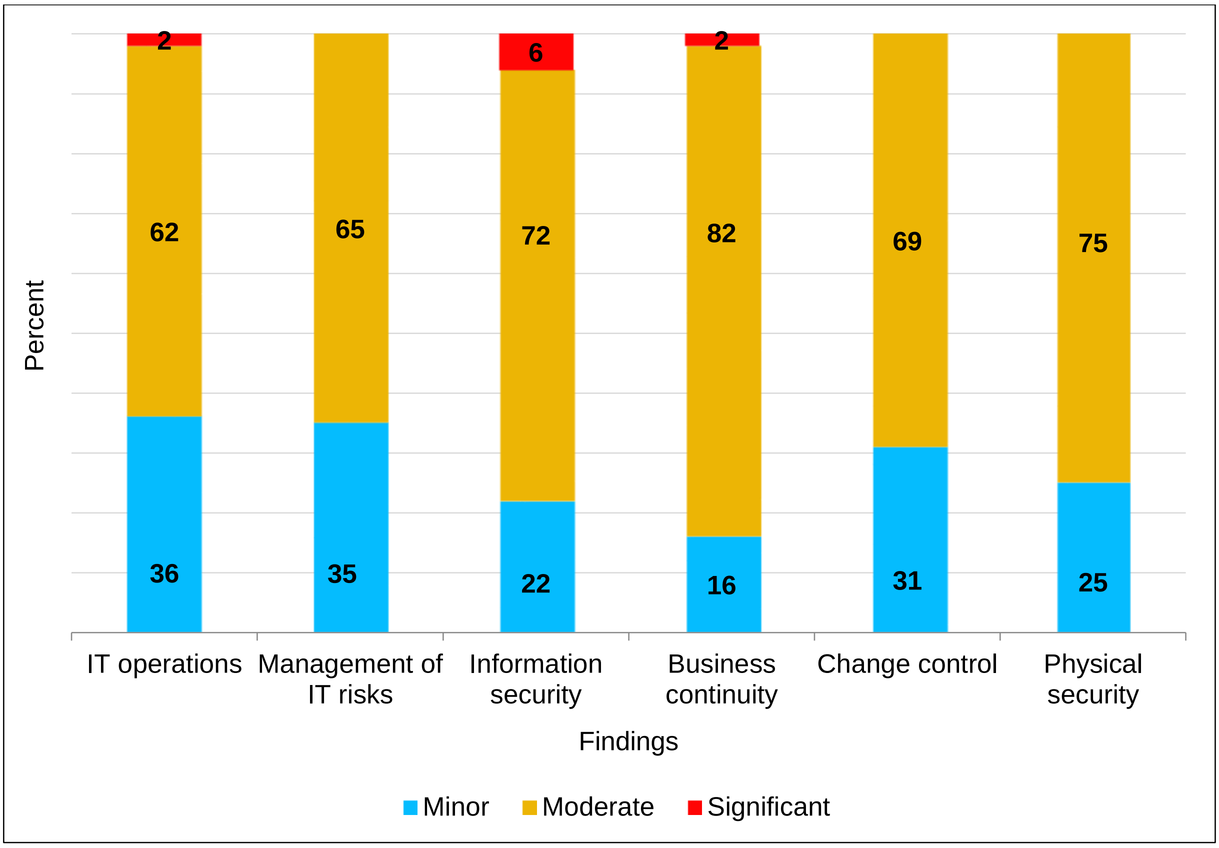
Weaknesses we observed included:

- no restricted access to computer rooms for staff, contactors and maintenance
- power generators in the event of power failure not tested
- no fire suppression system installed in the server room.

Inadequate protection of IT systems against various physical and environmental threats increases the potential risk of unauthorised access to systems and information and system failure.

The majority of our findings require prompt action

Figure 11 provides a summary of the distribution of significance of our findings. It shows that the majority of our findings at agencies are rated as moderate. This means that the finding is of sufficient concern to warrant action being taken by the entity as soon as possible. However, it should be noted that combinations of issues can leave agencies with more serious exposure to risk.



Source: OAG

Figure 11: Distribution of ratings for the general computer controls findings in each area we reviewed

Recommendations for GCC

1. As a matter of priority, agencies should address risks to security and continuity of business systems. In particular:

a. Information security

Executive managers should consider the ease with which systems could be compromised by referring to the case studies and should ensure good security practices are implemented, up-to-date and regularly tested and enforced for key computer systems. Agencies should conduct ongoing reviews of user access to systems to ensure they are appropriate at all times.

b. Business continuity

Agencies should have a business continuity plan, a disaster recovery plan and an incident response plan. These plans should be tested on a periodic basis.

c. Management of IT risks

Agencies need to ensure that IT risks are identified, assessed and treated within appropriate timeframes and that these practices become a core part of business activities and executive oversight.

d. IT operations

Agencies should ensure that they have appropriate policies and procedures in place for key areas such as IT risk management, information security, business continuity and change control. IT strategic plans and objectives support the business strategies and objectives. The OAG recommends the use of standards and frameworks as references to assist agencies with implementing good practices.

e. Change control

Change control processes should be well developed and consistently followed for changes to computer systems. All changes should be subject to thorough planning and impact assessment to minimise the likelihood of problems. Change control documentation should be current, and approved changes formally tracked.

f. Physical security

Agencies should develop and implement physical and environmental control mechanisms to prevent unauthorised access or accidental damage to computing infrastructure and systems.

Auditor General's reports

Report number	2018 reports	Date tabled
13	Management of Crown Land Site Contamination	27 June 2018
12	Timely Payment of Suppliers	13 June 2018
11	WA Schools Public Private Partnership Project	13 June 2018
10	Opinions on Ministerial Notifications	24 May 2018
9	Management of the State Art Collection	17 May 2018
8	Management of Salinity	16 May 2018
7	Controls Over Corporate Credit Cards	8 May 2018
6	Audit Results Report – Annual 2017 Financial Audits and Management of Contract Extensions and Variations	8 May 2018
5	Confiscation of the Proceeds of Crime	3 May 2018
4	Opinions on Ministerial Notifications	11 April 2018
3	Opinion on Ministerial Notification	21 March 2018
2	Agency Gift Registers	15 March 2018
1	Opinions on Ministerial Notifications	22 February 2018

OAG
Office of the Auditor General
Serving the Public Interest

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