Western Australian
Auditor General's Report

Information Systems Audit Report 2019

Report 20: May 2019

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 2019

Report 20
May 2019

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

INFORMATION SYSTEMS AUDIT REPORT 2019

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 public sector entities 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 entities included in our audits.

CAROLINE SPENCER
AUDITOR GENERAL
15 May 2019

Contents

Auditor General's overview

This is the eleventh annual *Information Systems Audit Report* by my Office. The report summarises the results of the 2018 annual cycle of information systems audits, and application reviews completed by my Office since last year's report.

The report contains important findings and recommendations to address common system weaknesses that can seriously affect the operations of government and potentially compromise sensitive information held by entities. All public sector entities should consider the relevance of the recommendations to their unique operations. The newly funded Office of Digital Government has an important role in supporting entities to address these weaknesses and improve their capability and cyber resilience.

The first section of the report contains the results of our audit of key business applications at 4 public sector entities. All 4 had weaknesses, the most common of which related to poor contract management, policies, procedures and information security.

When government outsources any ICT function, or buys cloud hosted applications, it remains responsible for identifying risks and ensuring appropriate functionality, security and availability controls are in place. Proper due diligence processes must be undertaken, when designing the contract and throughout the term of the contract, to ensure government gets the service it needs and the community expects. The potential effect of any weaknesses includes the compromise of sensitive information. Our Software as a Service (SaaS) better practice principles at Appendix 1 can assist entities in assessing whether to move to the cloud, choosing a provider and with ongoing contract management.

The second section presents the results of our general computer controls and capability assessments and I have identified 4 entities that have consistently demonstrated good practices over at least the past 3 years. I was pleased to find that 3 more entities were assessed this year as having mature general computer control environments across the 6 control categories of our assessment. However, the 2 categories of information security and business continuity, continue to show little improvement in the last 11 years. Despite a slight increase in the number of entities assessed as having mature business continuity controls, half of the entities we reviewed still do not manage this area well.

Ensuring good security practices are implemented, enforced and regularly tested should be a focus and key responsibility for all entities' executive teams. Continually raising staff awareness, at all levels, about information and cyber security issues is another proven way to embed good practice and security hygiene into everyday operations.

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 entities rely on to deliver services. We focus on the key controls that ensure data is complete, 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. Entities can use our better practice principles at Appendix 1 to help ensure any Software as a Service (SaaS) contracts include measures to mitigate risks and protect entity information.

Audit focus and scope

We reviewed key business applications at a number of state government entities. Each application is important to the operations of the entity and may affect stakeholders, including the public, if the application and related processes are not managed appropriately.

The 4 applications covered in this report are:

1. **Recruitment Advertisement Management System** – Public Sector Commission
2. **Advanced Metering Infrastructure** – Horizon Power
3. **Pensioner Rebate Scheme and Exchange** – Office of State Revenue
4. **New Land Register** – Western Australian Land Information Authority

Our application reviews focused on the systematic processing and handling of data in the following control categories:

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

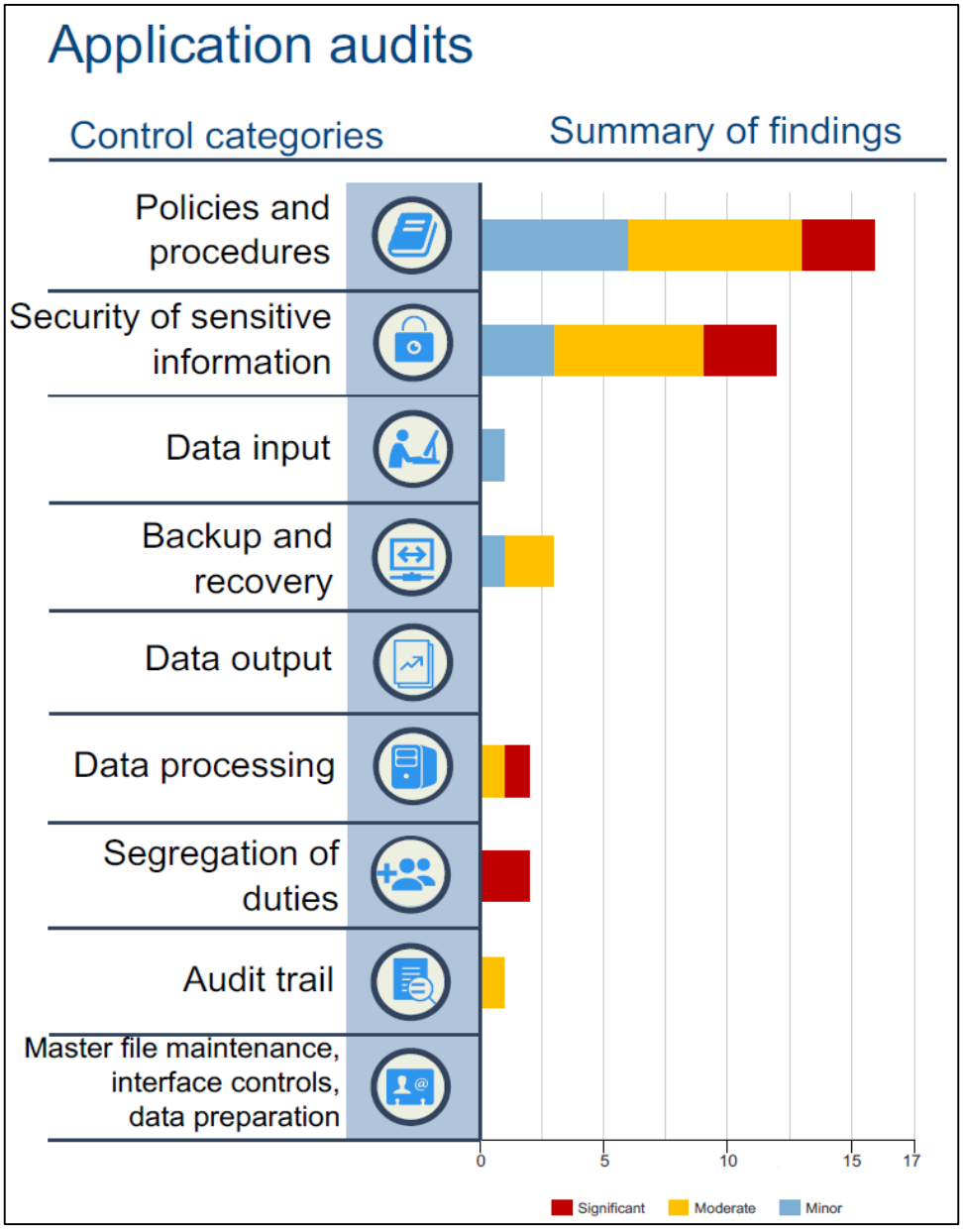
Our testing was a point in time assessment. We reviewed a sample of key controls and processes to obtain reasonable assurance that the applications worked as intended and that information they contained and reports were reliable, accessible and secure. Our testing may

highlight weaknesses in control design or implementation that increase the risk that an application's information may be susceptible to compromise. However, we do not design our tests to determine if information has been compromised.

Summary

The 4 applications we reviewed all had control weaknesses. Most related to policies and procedures, and poor information security. We also found weaknesses in controls aimed to ensure the applications function efficiently, effectively and remain available. We reported 37 findings across the 4 applications. Nine findings were rated as significant, 17 moderate and 11 minor.

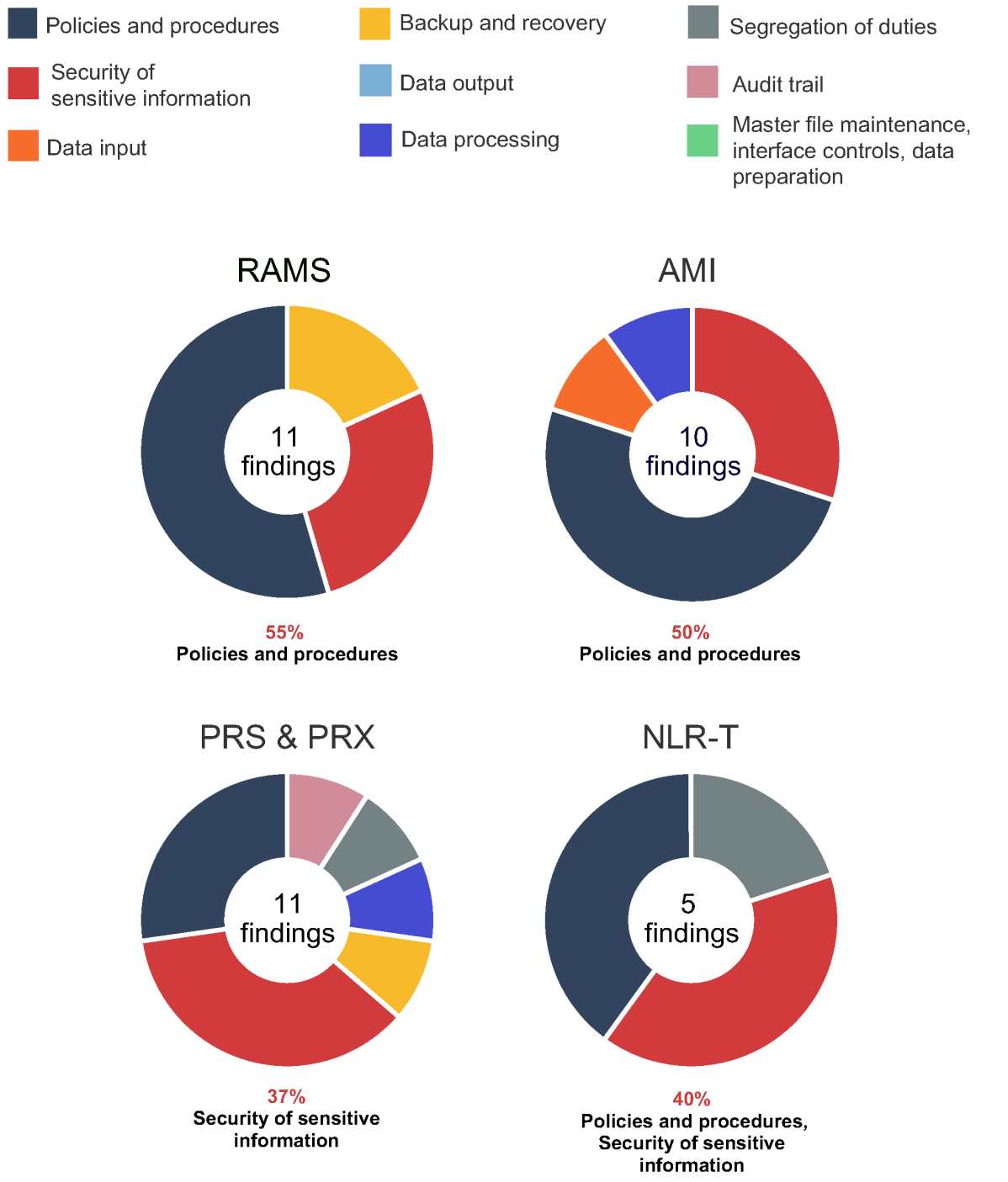
Most of the issues we found are relatively simple and inexpensive to fix. Figure 1 shows the findings for each of the control categories and Figure 2 shows the findings for each of the 4 applications reviewed.



Source: OAG

Figure 1: Application audits

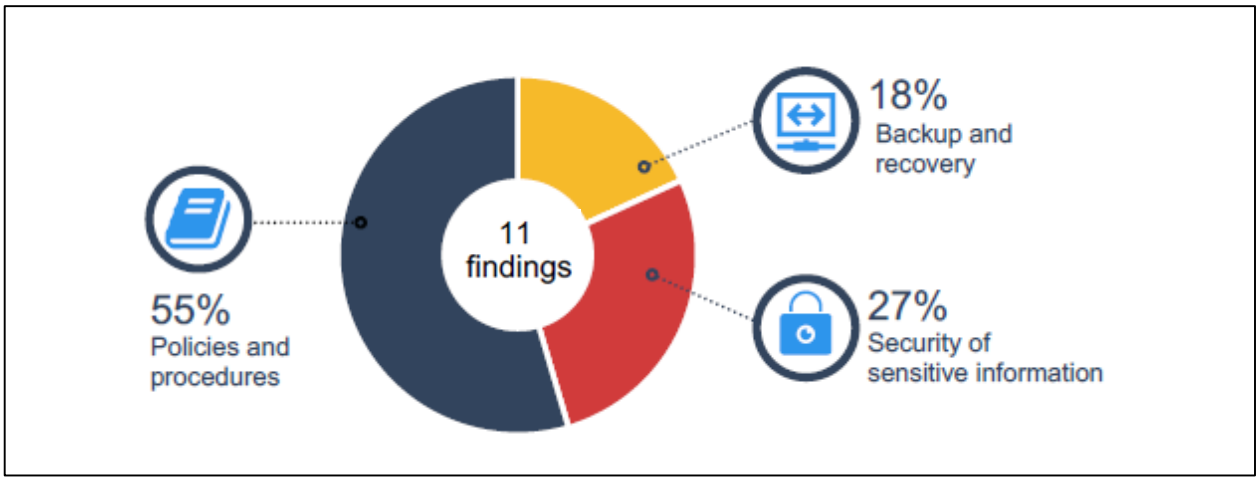
Findings per application



Source: OAG

Figure 2: Findings per application

Recruitment Advertisement Management System – Public Sector Commission



Introduction

Western Australian (WA) government entities use the Recruitment Advertisement Management System (RAMS) to manage staff recruitment and redeployments, and to record severance details. The public use the system to apply for WA government jobs. The system is externally hosted, and managed by a third-party vendor in a Software as a Service (SaaS) arrangement. It contains personal identifiable and sensitive information such as names, addresses, work history, qualifications, bank details and tax file numbers.

Conclusion

RAMS has successfully facilitated a significant number of recruitment processes since the application was implemented in 2003. However, we identified a number of opportunities to improve application governance. The Public Sector Commission (the Commission) has not undertaken or received independent assurance that key vendor managed information security controls are adequate and operating to ensure the confidentiality, integrity and availability of information in RAMS.

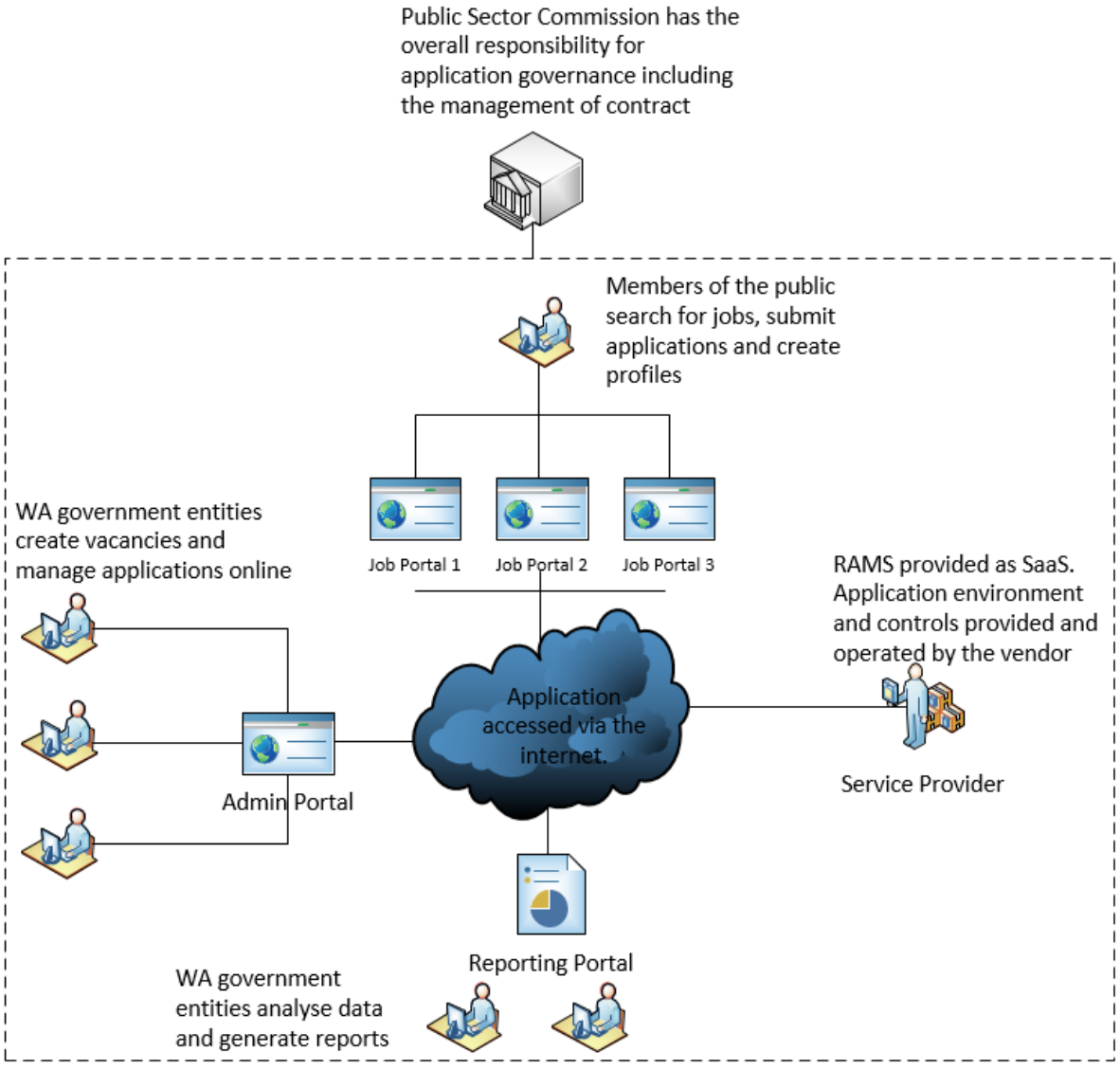
Further, the Commission cannot demonstrate it is monitoring and managing vendor compliance in accordance with the service level agreement and so may not be fully informed of any issues with service delivery or not meeting all users' needs.

There is also a risk that insufficient business continuity planning could see an outage impacting recruitment activities across the whole of the WA government.

Poor user access management has the potential to expose personal and sensitive information to inappropriate access or misuse, particularly as the Commission has kept all information stored on the system since 2003.

Background

RAMS is a mandated whole of government e-recruitment solution. All relevant WA state entities must use the application to advertise vacancies, manage redeployments and record severances. Entities access the application via an internet administration portal. A separate portal is provided for data analysis and reporting. The public can view vacancies, create a profile and submit job applications online through multiple job boards (Figure 3).



Source: OAG

Figure 3: High-level overview of RAMS

In 2017-18, RAMS processed about 238,000 applications for almost 15,400 job advertisements. Currently, there are about 712,000 people with a job seeker profile in the application.

The vendor manages the underlying environment (network, storage, servers, virtualisation, operating systems, middleware, runtime, data and applications) and controls to protect the system.

The Commission retains ownership of the data and the risks to its confidentiality, integrity and availability (Figure 4). It is also responsible for monitoring delivery of service as per the SaaS contract arrangement.

Security responsibility	Software (as a service)
Governance	Entity
Data	Entity and Vendor
Runtime	Vendor
Middleware	Vendor
Operating Systems	Vendor
Virtualisation	Vendor

Servers	Vendor
Storage	Vendor
Network	Vendor
Data Centres	Vendor

Source: OAG based on RAMS contract and SaaS principles[1]

Figure 4: SaaS security responsibilities

The WA public sector has used RAMS since 2003. The most recent contract extension was awarded in April 2018 for 2 years. A service level agreement is in place that sets out expectations of service.

Audit findings

The Commission has not sought adequate assurance on vendor controls

The Commission has not undertaken or received independent assurance that key vendor managed information security controls are adequate and operating effectively. As a result, the Commission does not have assurance that information in RAMS is protected to ensure its confidentiality, integrity and availability.

We identified the following control deficiencies:

- **Unsupported software** – Some software components that underpin the application are no longer supported by the software vendors. In addition, 1 component has not had software updates applied that fix known security vulnerabilities. Unsupported and out–of-date software increases the risk of attackers using known vulnerabilities to gain access to sensitive information or disrupt systems.
- **Disaster recovery not tested** – The vendor has not performed a full disaster recovery test since 2015. The Commission cannot be certain that it can recover the application as required.
- **Outdated technical specification documentation** – The technical documentation describing the application does not reflect the current application environment. The Commission cannot be certain that all appropriate controls are in place to protect the application.

Lack of a risk assessment has led to inadequate information security requirements in the contract

The Commission did not assess the information security risks to the RAMS application and information at the time of contract or extensions. Without a formal risk assessment, the Commission is less likely to know if controls documented in the contract adequately address risks and vulnerabilities. In a SaaS environment, the customer does not directly manage the controls that protect information. Therefore, it is critical that controls are well defined in the service contract.

We found key terms and conditions for security of information are inadequately specified in the contract.

Weaknesses we identified include:

- **No right to conduct security audits –** There is no specific right for the Commission to conduct security audits of the RAMS environment. As a result, the Commission may have limited ability to verify security controls.

[1] https://cloudsecurityalliance.org/download/security-guidance-v4/

- **No controls assurance –** There is no requirement for the vendor to provide the Commission with third party assurance reports or certification that controls are in place and operating effectively. The Commission cannot be certain that RAMS and the information it holds are protected.
- **Unspecified obligation to report data security breaches –** The vendor's obligation and process to report data security breaches to the Commission have not been specified. In addition, there are no defined penalties or indemnities for a security breach. Defining these requirements would allow the Commission to act in a timely fashion and, if necessary, recover costs in the event of a breach.
- **Encryption not specified –** Data encryption requirements to protect sensitive information in transit, at rest and stored on backups have not been specified. For example, the vendor does not encrypt backup tapes which are stored by a third party offsite. If the tapes are lost or stolen the information on them could be inappropriately accessed. The international standard for information security (ISO27002/2015) advises data owners to encrypt backup media where confidentiality is important.
- **Unspecified data retention –** Data retention requirements have not been specified. All information since 2003 has been retained in the system. This information is vulnerable to exposure if the application is compromised. Further, retaining all this information increases the risk that Australia's *Privacy Act 1988* and the European General Data Protection Regulation may be breached, which could result in infringements and reputational damage.

  The contract should also be consistent with the State Records Office's General Disposal Authority. This states that job applicant information should be disposed after 7 years for successful applicants and 1 year for unsuccessful applicants.

Inadequate access controls increase the risk of unauthorised access or misuse

We identified the following weaknesses in access controls to minimise the risk of unauthorised access:

- **Ineffective user account management –** The Commission does not have a policy or a procedure to manage entity user accounts, including highly privileged accounts. In addition, there is no process to routinely review user activity and their levels of access. There is an increased risk of unauthorised access to, or misuse of, information in the application.

  Ineffective user account management may have contributed to the high number of enabled accounts (approximately 30,000). 26% of these (8,000 accounts) have never been used and 50% (15,000 accounts) have not been used in over 6 months.
- **Weak password configuration –** The 'admin' portal does not meet good practice requirements for password complexity and does not limit the re-use of passwords. In addition, multi-factor authentication, where user access is only granted after successful presentation of 2 or more pieces of information, is not required to access the application. This leaves the portal susceptible to password guessing attacks and unauthorised access to information.
- **Unmanaged generic accounts –** Fifty five entities use generic accounts to access the internet facing reporting portal and the password for the generic account is easy to guess. Generic accounts and passwords are shared by email and the Commission does not know who has been given this information. As the password is easy to guess and not changed on a regular basis, staff moving within or leaving an entity may retain access to the reporting portal, increasing the likelihood of unauthorised access and disclosure.

Inadequate business continuity arrangements

We identified the following weaknesses in the Commission's business continuity arrangements that increase the risk that RAMS may not be restored in a timely manner after a disruption:

- **Out of date business continuity plan –** The Commission has not reviewed the RAMS Business Continuity Plan since 2014. Further, stakeholder entities' critical functions, processes and their recovery objectives were not considered during the 2014 business impact analysis. There is an increased risk that RAMS may not operate adequately during an incident and key stakeholder recovery requirements have not been specified in the vendor service contract.
- **Ineffective escrow management –** A software escrow agreement is in place, but the vendor has not deposited the code, data or documentation as required by the contract. The Commission was not aware of this since it had not verified the deposits to confirm that RAMS can be recovered from escrow. Without escrow deposits, the Commission will not be able to recover and continue the use of RAMS if the vendor can no longer provide the services.

  A software escrow helps protect all parties in a software license by having a third party (escrow agent) hold application source code, data and documentation. It ensures the Commission has access to a copy of the system, under certain contractual conditions.

Vendor compliance has not been well monitored to ensure RAMS meets entities' needs

We identified weaknesses in how the Commission manages the service level agreement (SLA). These increase the risk that the Commission will not receive the contracted services, or be aware of issues with the vendor's service delivery.

In particular, the Commission has not implemented key requirements of the SLA to manage the contracted service delivery. For example, the Commission has not:

- held annual contract review and periodic contract management meetings
- established, or allocated, a governance body to support forward planning and provide feedback on vendor performance
- conducted annual user satisfaction surveys since 2013
- received application backup reports and capacity management plans from the vendor.

We note that the Commission does hold quarterly and ad hoc meetings with the vendor. The Commission informed us that the 3rd quarter meeting is considered to be the annual review of the contract. However, we found no documentary evidence of an annual contract or SLA review in our examination of the most recent 3rd quarter meeting agenda or minutes.

Important application management processes could be improved to reduce the risk of unplanned system downtime

The Commission and vendor have not adequately documented, and do not routinely follow, change and incident management processes to manage issues with the application (e.g. incidents). Inadequate change and incident management can lead to unplanned system downtime and recurring issues. We identified the following weaknesses:

- **Changes are not properly managed –** Change management documentation is unclear and inconsistent. In addition, the vendor had not provided detailed change

process documentation as required by the SLA. We tested 2 changes which identified that:

- the formal contract change template is not used
- written confirmation of regression testing, to confirm changes have not negatively affected existing functions, and user acceptance testing is not performed.

- **Incidents are not properly recorded, classified and analysed –** The Commission does not record incidents and service requests in an appropriate service desk tool, increasing the risk that incidents may not be resolved in a timely manner.

  We note that the vendor does provide the Commission with incident volume reports. However, we found that incidents are not classified to allow trend analysis, and there is no documented process for identifying the root cause of recurring incidents. There is an increased risk that recurring incidents may not be identified and addressed.

Recommendations

The Commission should:

1. implement a risk assurance framework for SaaS arrangements and conduct a risk assessment of the RAMS application and information. Update contractual terms based on identified risks

   Commission response: Agreed

   Implementation timeframe: by December 2019

2. implement appropriate mechanisms and processes to manage and monitor SLA contractual obligations

   Commission response: Agreed

   Implementation timeframe: by December 2019

3. establish a suitable mechanism for obtaining feedback from stakeholders in key entities

   Commission response: Agreed

   Implementation timeframe: by July 2019

4. implement appropriate user account management practices and communicate these to all entities

   Commission response: Agreed

   Implementation timeframe: by October 2019

5. review and update the RAMS Business Continuity Plan based on an appropriate Business Impact Analysis involving key stakeholders, and update contractual availability requirements, if required.

   Commission response: Agreed

   Implementation timeframe: by December 2019

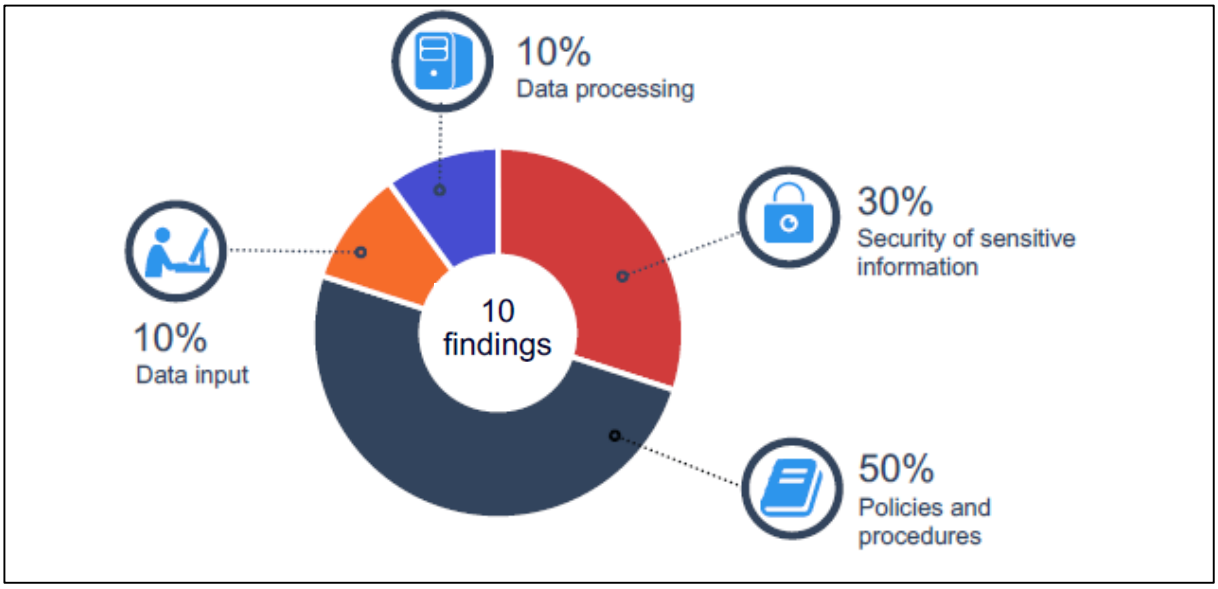
Response from the Public Sector Commission

The Commission notes the feedback and recommendations provided and undertakes to implement these recommendations.

The current whole-of-government e-recruitment system (RAMS) has had no security breaches since its inception in 2003. The Commission is confident that users' information is protected to ensure its confidentiality, integrity and availability.

The information provided in the audit will assist the Commission in enhancing the management of this contract, and will guide its future contractual requirements relating to information technology security as well as its auditing and application control requirements.

Advanced Metering Infrastructure – Horizon Power



Introduction

Our audit focused on the applications within the Advanced Metering Infrastructure used by the Regional Power Corporation, trading as Horizon Power (Horizon), to record, monitor and bill for the consumption of electricity. The applications store personal and sensitive client information such as customer name, address, date of birth and locations where electricity meters are installed.

Conclusion

The AMI system achieves its purpose. It collects and stores electricity consumption data and communicates the information to other Horizon business systems.

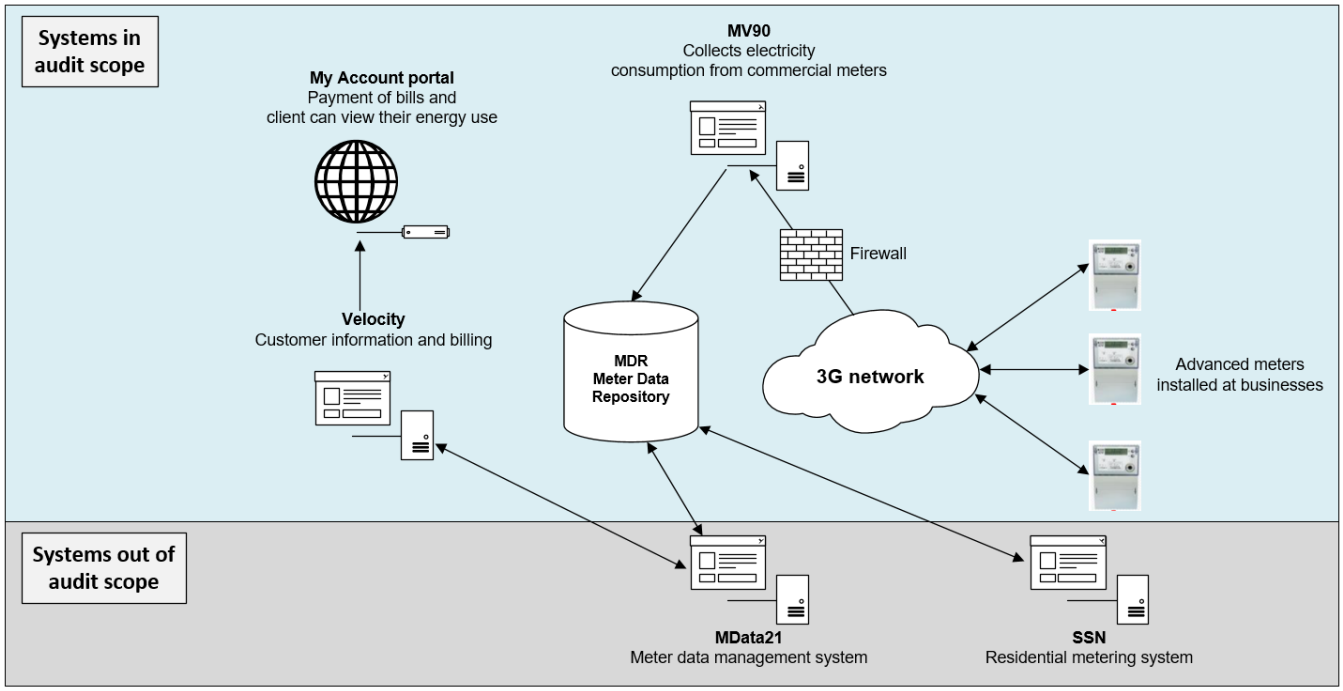
However, the integrity and confidentiality of the system and information it holds is at risk due to inadequate background checks and contractor access management. Improved network and database security controls would also strengthen system integrity.

Background

Horizon, is a state government-owned corporation that generates, procures and distributes electricity to residential, industrial and commercial customers in regional towns and remote communities. Currently it provides electricity to over 100,000 residents and 10,000 businesses.

Horizon has a suite of applications to manage electricity consumption and billing. Together, they are referred to as Advanced Metering Infrastructure (AMI). These include the MV90, Velocity, MDR, MData21 and SSN systems. Our audit focused on the MV90 commercial metering system, and associated applications including the ‘My Account’ portal.

The following figure (Figure 5) shows an overview of information flow across the different parts of the AMI system.



Source: OAG based on Horizon system flows

Figure 5: High level view of AMI system

In October 2016, more than 47,000 ageing electricity meters across regional WA were replaced with advanced meters. These meters allow Horizon to use the MV90 and other systems to collect electricity consumption data over the network without staff having to physically visit customer sites.

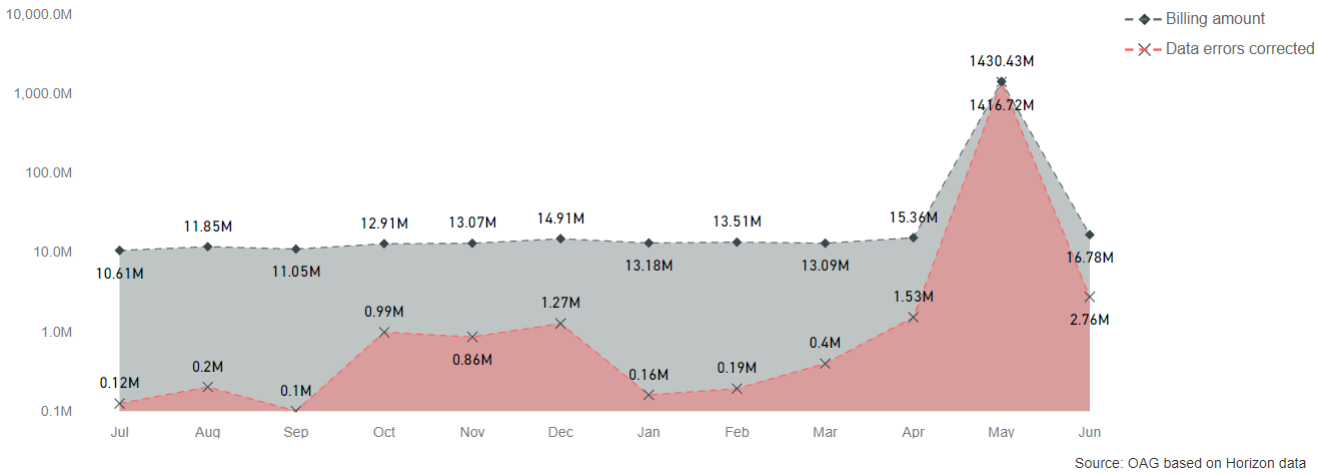
Audit findings

There are appropriate processes to detect and remedy consumption errors before bills are issued, but the value of errors is high

Horizon has good processes to detect and remedy data errors in consumption readings. Consumption readings occur daily for all advanced meters with network access. The Velocity system reports significant billing variances for early corrective action where required, and account managers review bills before they are issued to commercial customers.

In 2017-18, Horizon corrected errors valued at $1.43 billion (Figure 6). These comprised errors of $1.42 billion for one commercial customer and $8.5 million for other commercial customers. The $1.42 billion error arose from the manual reading of the customer's meter which does not have network access and must be read using a handheld device. Remaining errors were due to factors such as incorrect rates being applied to a customer, incorrect data and system changes.

While Horizon resolves errors as they arise, their high value is concerning.



Source: OAG based on Horizon data

Figure 6: Data errors corrected in FY 2017-18

Inadequate human resource security and contractor access management

Horizon's policies and processes do not require criminal history checks to be undertaken for staff. We found new staff employed without criminal history checks had privileged access to critical power infrastructure and systems. Additionally, regular background checks for key staff are not undertaken. Although recruitment processes include checks of references and qualifications, and medical tests, the process does not include criminal history checks. Without appropriate screening processes, staff may be assigned to positions of trust for which they are unsuitable.

We reviewed screening checks for 9 key staff and found 8 had not undergone adequate screening despite being in their roles for 3 to 14 months. This finding is concerning as these staff have privileged access to the network electricity management and other key systems.

We also found that Horizon's access management for third party contractor staff is not effective due to inaccurate HR records. Our review of 6 enabled contractor accounts found 3 belonged to former contractors who left Horizon 1 to 3 months before. Horizon has outsourced most of its ICT functions and over 300 contractors have been given access to the network and key systems to perform their work. Without an effective process to revoke contractor access, there is an increased risk that these accounts could be used to attack Horizon's IT network and systems.

We noted that Horizon does perform quarterly reviews of network access to identify and disable accounts that have not been used for 60 days. However, between reviews, contractors no longer working for Horizon can retain access to the network and systems.

System information is at risk of errors and unintentional disclosure

Horizon relies on manual forms to record important meter installation information before the information is entered in the applications. Manual workflows increase the risk of inaccurate information being entered into the applications. While Horizon informed us that a process to validate data entered from forms into the applications is in place, it is not clear if the process is carried out due to lack of documentation. Data errors will go unnoticed and impact the integrity of information if a data validation process is not consistently followed.

These forms also contain sensitive information such as property addresses and meter configuration details, including internet protocol (IP) addresses. We also found an instance of a Horizon staff member using a private email account to transmit this sensitive information to Horizon. The use of a private email account to transmit sensitive information increases the

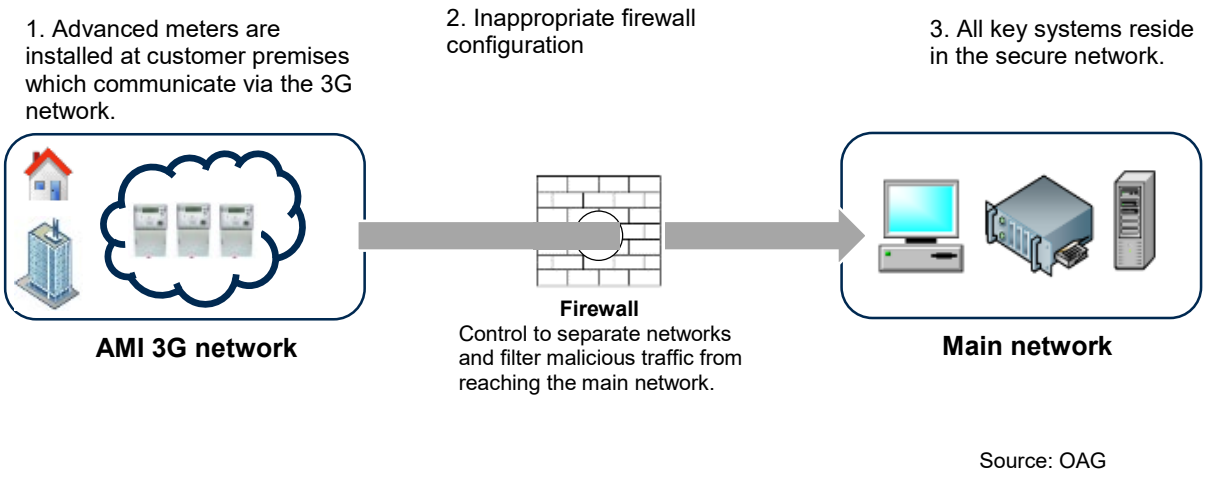
risk of unintentional disclosure. Horizon could improve the confidentiality and integrity of its information by implementing processes to collect data electronically.

There is room to improve security of the network and electronic records

Horizon's network and database security controls do not fully protect the confidentiality, integrity and availability of information. Weaknesses we found include:

- **Inappropriate configuration of the network firewall** – The firewall that separates the AMI network from Horizon's main corporate network was not properly configured (Figure 7). This increased the risk of cyber-attacks and unauthorised access to Horizon's key systems. Horizon has since addressed this issue.

  We also found that the firewall software was out-of-date. Software updates which addressed security vulnerabilities and performance issues had not been installed. This led to performance issues with the firewall and leaves the networks vulnerable to exploitation. Horizon has started work to update the firewall software.



Source: OAG

Figure 7: Inappropriate firewall configuration leaves security gaps

- **Database security is weak** – A number of security weaknesses render AMI databases vulnerable to unauthorised and inappropriate access compromising the confidentiality, and integrity of information in the databases.
  - AMI databases are not segregated to restrict and protect information from unauthorised access. Additionally, network users could access the databases due to a network policy error. Good practice suggests only those systems and users that need access should have access to databases.
  - Two databases had not had patches installed for 2 years and were missing 12 software updates, released to address security and performance issues. The risk that vulnerabilities will be exploited is increased when patches are not applied in a timely manner.
  - Personal information such as names, addresses, dates of birth, and gender are not encrypted to reduce the risk of the information being inappropriately used. Encryption increases the security of sensitive information and reduces the risk of inappropriate access.
  - Nine database accounts had not applied the password policy to enforce strong passwords. Weak passwords increase the risk of unauthorised access to systems and information.

- One database had inappropriately assigned privileges to all users. This allowed users to access privileged functions and gain access to sensitive information.

- **Network access accounts are not well managed** – The password for the highly privileged 'Administrator' account has not been changed for an extended period. This is despite privileged accounts being among the most targeted by hackers because they allow high levels of access. We also found from a sample of 16 network access accounts that 9 belonged to former staff and contractors and had not been disabled. Three of these can access ICT systems remotely. Without appropriate controls there is an increased risk of unauthorised or inappropriate access to the whole network.

- **Weak web server configuration** – Our external vulnerability assessment of the 'My Account' web portal identified a number of security weaknesses. These weaknesses increase the risk of unauthorised access or unintentional disclosure of information. We identified:

  - 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.

  Members of the public can use the 'My Account' portal to pay bills, update personal details and track their electricity consumption. If sensitive information was inappropriately accessed or disclosed it may lead to reputational damage for Horizon and adversely affect members of the public. Horizon's test of the portal also identified similar vulnerabilities and work is underway to address these weaknesses.

- **Lack of logging and event monitoring policy** – A formal activity log and event monitoring policy is not in place. This increases the risk that monitoring will be inconsistent and not identify potential problems, trends or ongoing attempts to compromise systems and information. We found that Horizon has good processes to capture application and system transactions, and activity. A formal monitoring policy would significantly strengthen controls.

There is a mature vulnerability management program but weaknesses in this process leave systems and information at risk of exposure

Third party application patching processes are ad hoc and informal. As a result, we found vulnerabilities in a number of systems. Without effective processes to manage vulnerabilities in third party applications, there is an increased risk that vulnerabilities could be exploited. This may result in unauthorised access to sensitive data or a loss of system operation in the event of a cyber-attack.

We found that Horizon has a mature vulnerability management process. Assessments and cyber security penetration tests are carried out regularly to identify potential security weaknesses. While database and third party application vulnerabilities could be better managed, operating system patches are installed in a timely manner to address known vulnerabilities.

Recommendations

Horizon should:

1. Determine, and where necessary resolve, the causes of consumption reading errors

   Horizon response: Agreed

   Implementation timeframe: by December 2019

2. develop appropriate policies and procedures to conduct adequate staff and contractor background checks

   Horizon response: Agreed

   Implementation timeframe: by July 2019

3. review manual processes and consider the use of digital forms and processes

   Horizon response: Agreed

   Implementation timeframe: by July 2019

4. review and implement appropriate network and database security controls

   Horizon response: Agreed

   Implementation timeframe: by July 2019

5. review and implement appropriate user access management practices

   Horizon response: Agreed

   Implementation timeframe: by July 2019

6. enhance the vulnerability management process to include third-party applications.

   Horizon response: Agreed

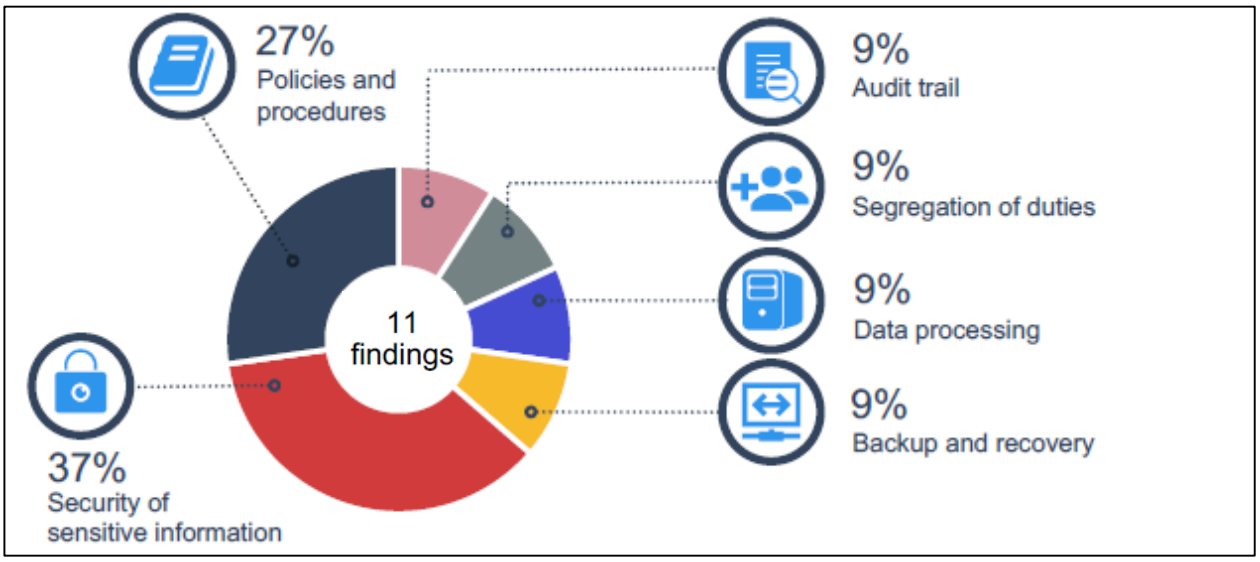
   Implementation timeframe: by July 2019

Response from Horizon Power

Horizon Power welcomes the application control and management review by the Office of the Auditor General (OAG). The results confirm a number of findings identified through internal assessments and provide additional areas for improvement. Horizon Power has agreed to all of the recommendations and has moved quickly to address all recommendations where reasonable. The confidentiality, integrity and availability of systems remains a focus for Horizon Power and audits conducted by the OAG assist in improving controls and governance across our environment.

1. Horizon Power is aware of the reasons for consumption data issues and advises that there is very limited practical ability to resolve these issues due to the complexity of Large Enterprise contract management and billing. Horizon Power agrees with the intent of the recommendation, and will continue to investigate issues and seek improvements but will need to continue to make manual bill adjustments related to contract conditions. It is pleasing that the OAG has noted the controls in place. Horizon Power also notes that no incorrect bills were issued as a result.
2. Horizon Power have implemented improvements to the employee and contractor on-boarding and off-boarding processes, including criminal history checks prior to appointment to positions of trust and regularly throughout the employment period.
3. Horizon Power will be assessing the costs and benefits of implementing a digital solution. In the meantime, Horizon Power has reinforced with employees the importance of the accuracy and confidently of data collected through manual forms.
4. Horizon Power has identified, reviewed and implemented improvements to remediate issues identified prior to, and during, the audit within the network and database security control environment.
5. Horizon Power has implemented the necessary improvements to user access management practices. The improvements have predominantly been within the employee and contractor on-boarding and off-boarding processes to ensure that user access is accurate and updated in a timely manner.
6. Horizon Power has conducted a review to identify any existing vulnerabilities within third-party applications. In addition, there have been improvements made to the patch management process in relation to third-party applications.

Pensioner Rebate Scheme and Exchange – Office of State Revenue



Introduction

The Office of State Revenue (State Revenue) process local government entities' (LGs) claims for reimbursement of concessions they pay to eligible pensioners and seniors through the Pensioner Rebate Scheme (PRS) system and its Pensioner Rebate Exchange (PRX) interface.

LGs use PRX to exchange claims information with State Revenue.

PRS and PRX were developed and are maintained by State Revenue.

Conclusion

The PRS and PRX effectively support State Revenue and LGs to process reimbursement claims. The rebate calculation process works well. However, State Revenue has not performed land ownership and occupancy checks since 2005. This increases the risk of concessions being paid to ineligible individuals.

Weak access controls and a lack of disaster recovery planning may also compromise the confidentiality, integrity and availability of information in PRS and PRX. State Revenue also does not effectively protect its systems from the threat of cyber-attacks.

Background

The State Revenue is a business unit of the Department of Finance. It collects duties and taxes, and administers several grants and subsidies paid to the community.

It also manages LG claims in line with the *Rates and Charges (Rebates and Deferments) Act 1992* (the Act). To be eligible for rebates and deferments on LG rates (sewerage, drainage and underground electricity) and emergency services levy charges, a person must:

- register with the Water Corporation or relevant Local Government as a pensioner or senior under the Act

- hold a pensioner or senior card. Pensioners receive up to 50% rebate and are allowed to defer payments; seniors receive up to 25% rebate
- own and occupy a residential property on 1 July of the claim year.

Section 36 of the Act requires that ownership, occupancy and eligibility information supplied by pensioners and seniors be confirmed every 3 years. LGs did these checks until 2003, after which State Revenue took over the responsibility on behalf of LGs.

State Revenue and the Department of Treasury share responsibility to reimburse LGs for rates, rebates and interest on deferred rates that arise from pensioner and senior concessions. State Revenue processes LG claims for reimbursement, checks eligibility and validates payment amounts. Treasury pays the money to LGs.

Claims are managed through the PRS system and the PRX interface. LGs submit reimbursement claims to State Revenue through the internet accessible PRX, after pensioners and seniors have paid their portion. State Revenue uses the PRS system to process LG claims. PRS and PRX hold confidential information, such as concession card numbers and personal details.

Over the period of July 2015 to June 2018, PRS processed an average of 469,000 claims each year, paid an average of 443,000 claims each year, and rejected an average of 26,000 claims each year. In 2017-18, State Revenue paid $117.2 million to LGs in reimbursements.

Audit findings

State Revenue does not perform land ownership and occupancy checks, which increases the risk of payments being made to ineligible individuals

State Revenue does not perform land ownership and occupancy checks as required by the Act. State Revenue took over this responsibility from LGs in 2003 but stopped doing the checks in 2005. Appropriate validation processes reduce the risk of incorrect concessions being paid to pensioners and seniors.

We were told by State Revenue that the checks stopped because a high number of payment claims were falsely rejected due to inaccurate land occupancy and ownership information in LG claim files and State Revenue records. State Revenue did not inform LGs that the checks had stopped until June 2018.

In 2010, we made a similar finding that PRS did not perform land ownership and occupancy checks against land records[2]. Over 15 years later, the function has not been fixed. State Revenue told us that it will now fix this by June 2019.

Inadequate controls may lead to unauthorised use of information

State Revenue does not have appropriate user access or security controls despite storing personal and confidential information in PRS and PRX. We identified the following weaknesses, which may compromise the confidentiality and integrity of information in the system:

- **Inadequate user access controls and reviews** – State Revenue does not regularly review PRS and PRX user accounts. We found an excessive number of user accounts with administrator privileges. Additionally, many PRX user accounts, including those with privileges, had not accessed the system for 12 months (Table 1). Administrator privileges allow high levels of access and are most targeted by attackers. Unused

[2] General Computer Controls Audit FY 2009-10

dormant accounts could be used for malicious activity. State Revenue started a review of PRX user accounts in August 2018, but it is limited to external LG users and does not cover internal State Revenue users.

System	Privileged users	Percent of user accounts that had not accessed the system for 12 months or more
PRX – State Revenue users	20 of 24	46%
PRX – LG users	194 of 294	7%
PRS	18 of 29	0%

Source: OAG based on State Revenue data

Table 1: Dormant user and privileged accounts

- **A large number of users have access to unprotected sensitive information** - We identified 60 users, including software developers, with full access to read, modify and delete pensioner eligibility reports and payment files. This increases the risk of unauthorised access and changes to information, and of fraudulent payments. We found:
    - payment files are in plain-text
    - the payment verification process in place is not adequate. It cannot detect if the payee account details in the payment file have been changed
    - pensioner eligibility reports and payment files are stored on a shared network folder without appropriate restrictions.

  Payment files are generated by State Revenue and contain the reimbursement amounts and LG payee bank account details. Pensioner and senior eligibility reports are provided to State Revenue by Centrelink, the Department of Veteran's Affairs and Department of Communities to identify eligible pensioners.

- **Easy to guess database passwords** - We identified 10 database accounts with easy to guess passwords, and 70 accounts that had not changed their passwords for over 12 months, as required by State Revenue's Password Policy. Seven of the 70 accounts had not changed their passwords for an extended period. Weak password controls increase the risk of unauthorised access to the system.

- **Segregation of duties** - We found 17 users were able to perform end-to-end steps in the claims process as they have access to both PRS and PRX. These users can submit claims, process claims and submit payment requests. It is a basic security principle that a person who initiates a process should not be the one to authorise it. Without adequate segregation of duties, there is an increased risk of unauthorised or fraudulent payments.

  18 of the 60 users with excessive privileges could also modify LG bank account details and email addresses in the PRS system without approval. The PRS system does not notify relevant LGs when sensitive information, such as bank account details, are amended. State Revenue and LGs may only become aware of unauthorised changes if LGs query non receipt of payments.

- **System activity is not adequately monitored or recorded** - State Revenue does not have a policy or adequate procedures to proactively monitor user activity and log changes to information in PRS and PRX. Without appropriate monitoring, State

Revenue may not detect inappropriate access or unauthorised changes. While user details and time of access are logged, there is no log of changes made to the information.

- **State Revenue has not developed an acceptable use policy** - Ninety-two percent of PRX users are from LGs but State Revenue has not developed an acceptable use policy to guide their use. An 'acceptable use policy' is a set of guidelines that outline terms and conditions for system use. It is good practice to develop these guidelines and make sure all users are aware and understand them. Without appropriate guidance, there is increased potential for inappropriate access and use of system.

Security vulnerabilities are not well managed, leaving PRS and PRX exposed to attack

There is insufficient security vulnerability management. We found:

- over 600 vulnerabilities on workstations due to unsupported third party applications and missing security updates (patches)
- state Revenue has not installed anti-malware software on the PRS production (live) server
- State Revenue does not have a process to identify vulnerabilities in PRS or PRX.

Vulnerabilities could be exploited by attackers to gain unauthorised access to sensitive data or interrupt State Revenue's business. Timely patching of software reduces the footprint for potential attacks.

State Revenue may not be able to recover PRS and PRX following a major incident or disruption

State Revenue does not have an information technology Disaster Recovery Plan for PRS and PRX. This could compromise the availability of the system following a major incident or disruption. State Revenue told us that Disaster Recovery Plans for other systems may help recover PRS and PRX, but it has not tested recovery.

State Revenue technical support documentation for PRS and PRX is not up-to-date and does not describe the current system environments. We found some documentation had not been reviewed since 2001. The State Revenue may not have the technical documentation to recover the system in the event of a major incident or disruption.

Recommendations

State Revenue should:

1. update its information security policy and processes to better manage user access

   State Revenue response: Agreed

   Implementation timeframe: by August 2019

2. reinstate validation of identity processes and checks of land ownership and occupancy in accordance with the Act

   State Revenue response: Agreed

   Implementation timeframe: by July 2019

3. establish processes to update system user support documentation

   State Revenue response: Agreed

   Implementation timeframe: by December 2019

4. develop and implement an effective framework to log and monitor key changes to PRX and PRS

   State Revenue response: Agreed

   Implementation timeframe: by December 2019

5. enhance the vulnerability management process to identify and address weaknesses

   State Revenue response: Agreed

   Implementation timeframe: by July 2019

6. develop and regularly review information technology Disaster Recovery Plans for PRX and PRS.

   State Revenue response: Agreed

   Implementation timeframe: by December 2019

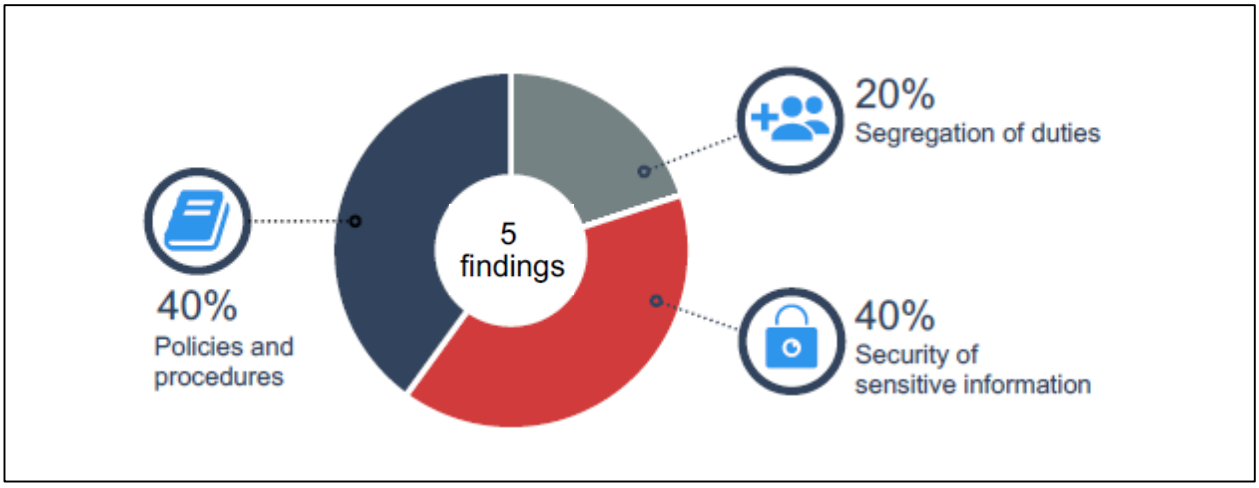
Response from the Office of State Revenue

The Office of State Revenue accepts the recommendations in the Summary of Findings and considers them achievable within the timeframes specified.

Progress has been made against all of the recommendations and it is expected that all of the implementation timeframes will be met.

The Office of State Revenue has been working to develop a system that will validate land ownership and occupancy information. This system has now been built and will be implemented by July 2019, with validations checks progressively rolled out to the 136 local government authorities.

New Land Registry - Titles – Western Australian Land Information Authority



Introduction

The New Land Registry – Titles (NLR-T) application is used by the Western Australian Land Information Authority, trading as Landgate, to manage property ownership and location information records for Western Australia. The NLR-T partially automates the previous paper-based land registration process. The NLR-T was developed and is maintained as part of an outsourced ICT arrangement using public cloud infrastructure. This arrangement is jointly managed by a Landgate subsidiary co-owned with a third party vendor.

Conclusion

The NLR-T application works as intended and allows Landgate to effectively manage land title transactions. However, Landgate's management of user access and information could be improved to protect the confidentiality and integrity of information in the NLR-T. Data verification and external network security reviews will further strengthen the security of the system and information.

Background

Landgate is one of the oldest state government entities. It manages property and land information and maintains the State's official register of land ownership under the *Transfer of Land Act 1893* (the Act).

Landgate uses the NLR-T to manage land title information, including transfers of ownership, mortgages, and discharge of mortgages. In 2017, the NLR-T processed over 1.4 million titles and $36.2 billion worth of transactions.

Prior to 2015, Landgate used the Smart Register system to manage land ownership. However, the aging technology became costly to maintain and lacked the flexibility needed to suit business needs.

The application was built by the jointly-owned subsidiary using modern principles and is maintained on a cloud platform. Implementation started in June 2015 and was completed in January 2017. The NLR-T was delivered in stages to minimise the impact on Landgate's business. The NLR-T replaced the old Smart Register system.

Government has announced its intent to partially commercialise Landgate's automated functions including the NLR.

Audit findings

Changes to land information are not reviewed

Landgate does not review transactions in the NLR-T for accuracy. It stopped these reviews in 2016. From a review of 8 land transactions in 2018, we identified 2 land title changes that were made without appropriate delegation. This increases the risk of erroneous or inappropriate changes to NLR-T information, and is a breach of the Act. However, we found the 2 transactions had appropriate documentation to support the changes.

Inadequate user access controls could lead to unauthorised access or misuse of information

We found weak user access controls that pose an increased risk of unauthorised access and misuse of information given the NLR-T uses cloud infrastructure and is built for use by multiple tenants. Special attention should be given to how privileged access rights are managed. We identified weaknesses in the following areas:

- **Inadequate segregation of duties –** Two staff had been assigned excessive privileges allowing them to perform end-to-end land title transactions. It is a basic security principle that a person who initiates a request should not be the one to authorise it. Without adequate segregation of duties, there is an increased risk of errors not being detected and that unauthorised or fraudulent activities may occur and result in inappropriate changes to land title information
- **Excessive user access rights –** We found 7 users were granted 'Assistant Registrar' highly privileged user rights, which can be used to bypass system checks, when they only needed basic rights to perform their duties. The privileges were given due to there being no basic access role in the system
- **Irregular user access reviews –** User access rights and permissions are not regularly reviewed to confirm they are still required and appropriate. Over time this allows users to accumulate excessive privileges, potentially leading to unauthorised or inappropriate access to information. In 1 instance we found that a former Landgate employee still had access to the network and NLR-T system.

Lack of external Network Penetration testing may result in vulnerabilities going undetected

While Landgate performs internal vulnerability scans of application source code and infrastructure, it has not tested the adequacy and effectiveness of controls to detect and prevent external network attacks on the NLR-T since it went live. A failure of these controls may impact the confidentiality, integrity and availability of land information. These tests are particularly important as parts of the application are publicly accessible and reside in a shared cloud environment. Tests should be performed regularly to keep pace with evolving cyber threats.

Credit card data is at risk of exposure

Landgate is in breach of its own *ICT Acceptable Use Policy* which prohibits credit card details being stored using insecure methods, such as email. We found payment forms containing credit card information stored in long term backups without appropriate masking of the details.

Storing credit card details without appropriate levels of protection is also a breach of the *Payment Card Industry Data Security Standard*. The Standard sets guidelines and requirements for organisations that store credit card information. Landgate does have a process to ensure compliance with the Standard and provides training to staff that deal with credit card information, however the controls failed for this process.

Contracted IT services have not been reviewed

Landgate has not had its outsourced ICT services reviewed since the Master Agreement was signed in November 2016. The agreement recommended review of delivery and the cost of services after 12 months. Landgate does not know if the services being delivered meet contractual obligations.

It will be important in any future commercialised arrangements that Landgate maintains visibility of appropriate controls and obtains appropriate assurance over their ongoing effectiveness to protect the security and integrity of NLR-T data.

Recommendations

Landgate should:

1. review its access policies, procedures and controls to ensure they are implemented effectively

   Landgate response: Agreed

   Implementation timeframe: by July 2019

2. assess the risks around not performing land registry transaction reviews and ensure implemented controls align with this assessment

   Landgate response: Agreed

   Implementation timeframe: by July 2019

3. enhance the vulnerability management process to include external vulnerability assessments

   Landgate response: Agreed

   Implementation timeframe: by July 2019

4. establish appropriate controls to protect sensitive information, particularly credit card information

   Landgate response: Agreed

   Implementation timeframe: by July 2019

5. consider a review of delivery and the cost of services under the Master Agreement, and ensure appropriate controls and assurances are maintained in any future commercialised arrangement.

   Landgate response: Agreed

   Implementation timeframe: by July 2019

Response from Landgate

Landgate acknowledges the recommendations and has implemented changes to the business processes and practices that support the NLR-T to further enhance the access controls of the application and Landgate's overall ICT environment. All recommendations will be completed by June 2019.

Landgate has extended its security framework to further strengthen its infrastructure, taking additional steps to mitigate risks:

- ICT Security monitoring extended to 24/7 coverage;
- Additional vulnerability-detection software deployed to bolster internal testing;
- A provider for external penetration testing is currently being procured.

Access to NLR-T is now independently managed via Landgate's Service Now application ensuring an audit trail of access and approvals, including appropriate authorisation.
The recommendation regarding the protection of sensitive information, including credit cards, relates to a business control that is not specific to the NLR-T. Changes have been made to how Landgate captures the submission of customers credit card details with long-term back-ups now encrypted.

Landgate has renegotiated its Master Services Agreement with ICT service provider, Advara Ltd. The new agreement has been reviewed independently. The governance framework requires all services to be reviewed monthly for performance and delivery outcomes, with comprehensive service level agreement reporting.

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 2018 we focused on the following 6 control categories:

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

Conclusion

We reported 547 general computer controls issues to the 47 state government entities audited in 2018 compared with 539 issues at 47 entities in 2017.

There was a small increase in the number of entities that met our expectations across all 6 control categories. Thirteen entities met our expectations, compared with only 10 in 2018.

While system change controls and physical security are managed effectively by most entities, less entities met our expectations in these categories in 2018. The 2 categories of information security and business continuity continue to show little improvement in the last 11 years. We saw an increase in the number of entities with defined business continuity controls, but half of the entities we reviewed still do not manage this area well. The majority of issues we identified can be easily addressed with better information security management and keeping processes to recover data and operations in the event of an incident up to date.

By not prioritising the security and continuity of information systems, entities risk disruption to the delivery of vital services to the community and compromise the confidentiality and integrity of the information they hold. Embedding a security culture across all levels of an organisation is essential to building a cyber and information security aware workforce.

Background

We use the results of our GCC work to inform our capability assessments of entities. Capability maturity models are a way to assess how well developed and capable the established IT controls are. The model provides a benchmark for entity performance and means for comparing results from year to year.

The model we have developed uses accepted industry good practice as the basis for assessment. Our assessment of GCC maturity is influenced by various factors. These include: the business objectives of the entity; the level of dependence on IT; the technological sophistication of their computer systems; and the value of information managed by the entity.

Audit focus and scope

We conducted GCC audits at 47 state government entities. This is the eleventh year we have assessed entities against globally recognised good practice.

We provided 39 of the 47 entities with capability assessments and asked them to complete and return the forms at the end of the audit. We then met with each of the entities to compare their assessment and ours, which was based on the results of our GCC audits. Five entities, whose GCC audits were outsourced, were not included in the capability assessment. Three other entities are also not included as detailed work was not performed at these entities as a result of Machinery of Government changes.

We use a 0-5 rating scale[3] to evaluate each entities' capability maturity level in each of the GCC control categories. The model provides a baseline for comparing entity results from year to year. We have included specific case studies where information security weaknesses potentially compromise entities' 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 entity quick to adapt.

Source: OAG

Table 1: Rating scale and criteria

Audit findings

Our capability maturity model assessments show that entities need to establish better controls to manage information security, business continuity and IT risks. Figure 1 summarises the results of the capability assessments across all 6 control categories for the 39 entities we assessed. We expect entities to achieve a level 3 (Defined) rating or better across all the categories.

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

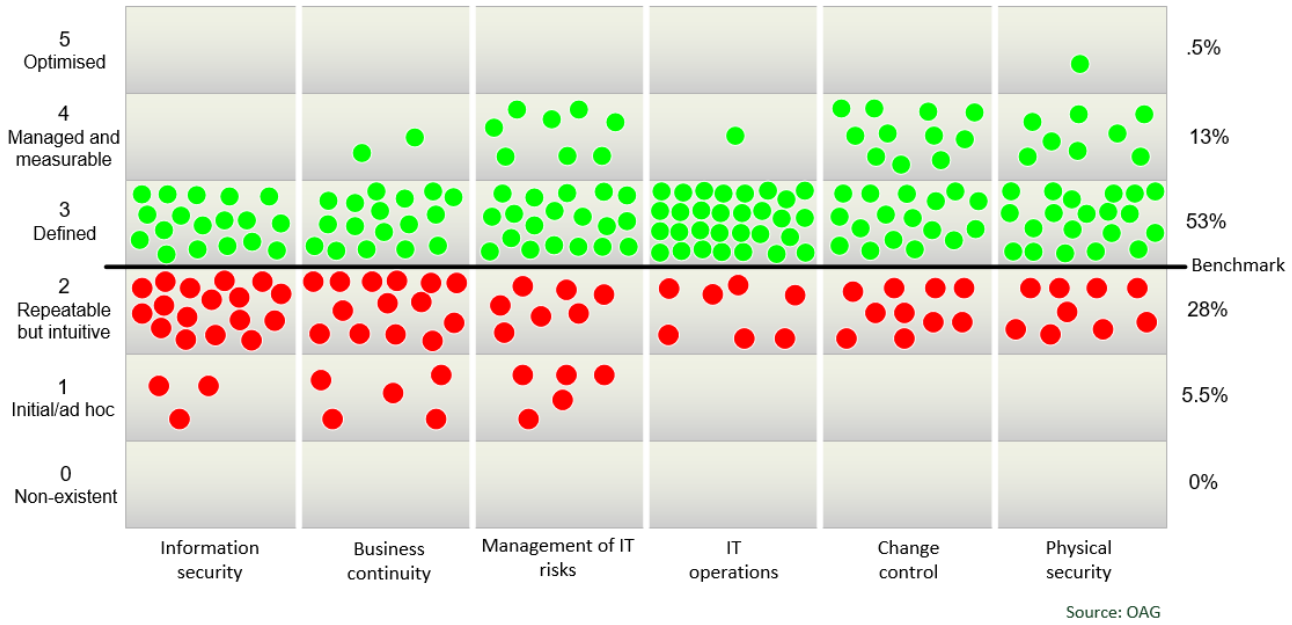


Figure 1: Capability maturity model assessment results

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

The percentage of entities rated level 3 or above for individual categories was as follows:

Category	2018 %		2017 %
Information security	47	↓	50
Business continuity	50	↑	37
Management of IT risks	69	↓	72
IT operations	82	↑	75
Change control	74	↓	84
Physical security	76	↓	90

Source: OAG

Table 2: Percentage of entities rated level 3 or above

The 2018 results show a decline in 4 of the 6 categories. Business continuity continued to show improvement, however, it is still of concern that only half of the entities were adequately controlled in this area.

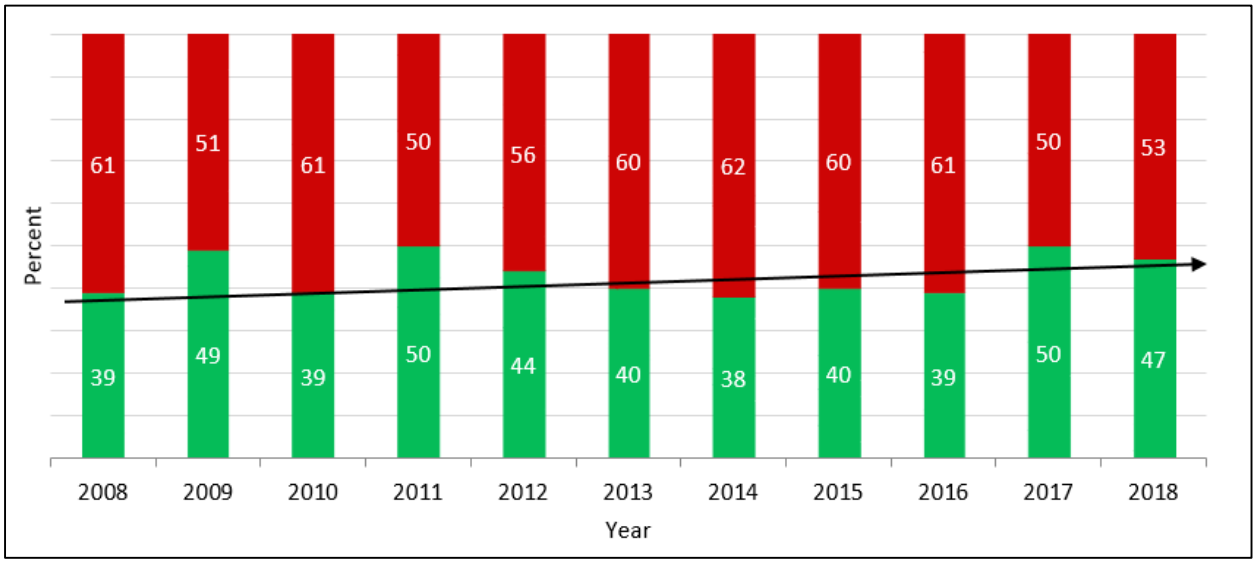
Of the entities we review every year there are only 4 that have consistently demonstrated good practices across all control categories assessed:

- Department of the Premier and Cabinet (6 years at level 3 or higher)
- Racing and Wagering Western Australia (5 years at level 3 or higher)
- Western Australian Land Information Authority (3 years at level 3 or higher)
- Curtin University (3 years at level 3 or higher)

Information security

Only 47% of entities met our benchmark for effectively managing information security in 2018. This represents a 3% decline from 2017. It is clear from the basic security weaknesses we identified that many entities lack some important security controls needed to protect systems and information. The trend across the last 11 years shows little improvement in entities' controls to manage information security.

We assessed whether entity 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 entities that met the benchmark and red represents the entities that did not meet the benchmark.

Weaknesses we found included:

- information security policies did not exist, were out of date or not approved
- intrusion detection/prevention system not configured leaving exposures
- lack of processes to upskill staff in information security
- no review of highly privileged application, database and network user accounts
- lack of processes to identify and rectify security vulnerabilities within IT infrastructure
- no information security awareness programs for staff
- easy to guess passwords for networks, applications and databases, e.g. Password, Password1.

Information security is critical to maintaining the integrity and reliability of information held in key financial and operational systems, and protecting them from accidental or deliberate threats and vulnerabilities.

The following case studies demonstrate the risks to entity information when information is not securely managed.

Critical vulnerabilities not addressed

In 2017-18 we performed vulnerability assessments and reported thousands of security vulnerabilities on a small sample of key systems at entities.

At one entity we found that network and IT systems were vulnerable due to lack of anti-malware and intrusion detection/prevention controls, and missing security patches. The entity had also not patched WannaCry vulnerabilities for over 5 months, and did not have a process to patch Linux environments with missing patches dating back to 2013.

Without an effective process to identify, assess and address relevant vulnerabilities in a timely manner there is an increased risk that systems will not be adequately protected against potential threats. These vulnerabilities could be exploited and result in unauthorised access to IT systems and information.

Figure 3: Vulnerabilities expose entity systems

Multifactor authentication is not implemented

Many entities access critical systems hosted in the cloud, including payroll and financial, over the internet without requiring additional controls such as multifactor authentication. Multifactor authentication adds a layer of security and is a good safeguard against unauthorised access to systems and information.

We also found some entities did not require multifactor authentication for remote access into their network and IT systems increasing the risk of unauthorised access to entity IT systems and information.

Figure 4: Internet accessible systems lack controls

Passwords stored in plain text

At one entity we found passwords stored in plain text on the shared network drive. These included database and server account credentials for a critical system.

A malicious user could read these credentials to gain unauthorised access to entity information. As a good practice, passwords should not be stored in plain text.

Figure 5: Storing passwords in plain text allows unauthorised access to systems

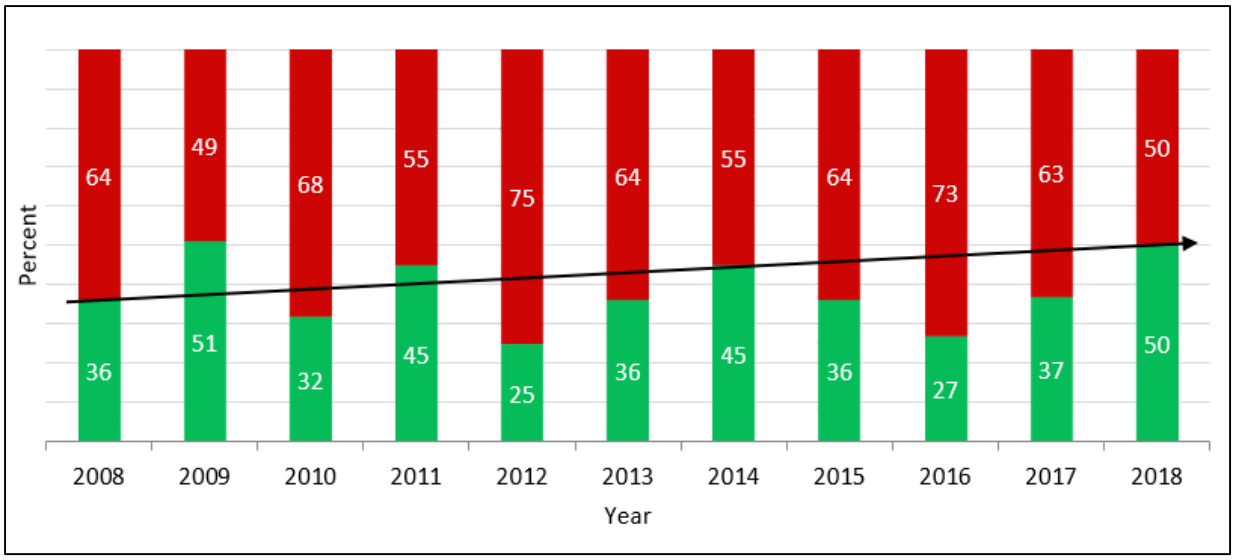
Continually raising staff awareness at all levels, about information and cyber security issues is a proven way to embed good practice and security hygiene into everyday operations.

Business continuity

To ensure business continuity, entities should have in place an up to date business continuity plan (BCP), disaster recovery plan (DRP) and 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 provides important rapid recovery of computer systems in the event of an unplanned disruption to business operations and services. Senior executives should monitor that plans are developed and tested in accordance with the risk profile and appetite of the entity.

We examined whether plans had been developed and tested. We found a 13% improvement from last year, however, 50% of the entities still did not have adequate business continuity and disaster recovery arrangements in place. The trend over the last 11 years has shown entities are not affording sufficient priority to disaster recovery and continuity.



Source: OAG

Figure 6: Business continuity

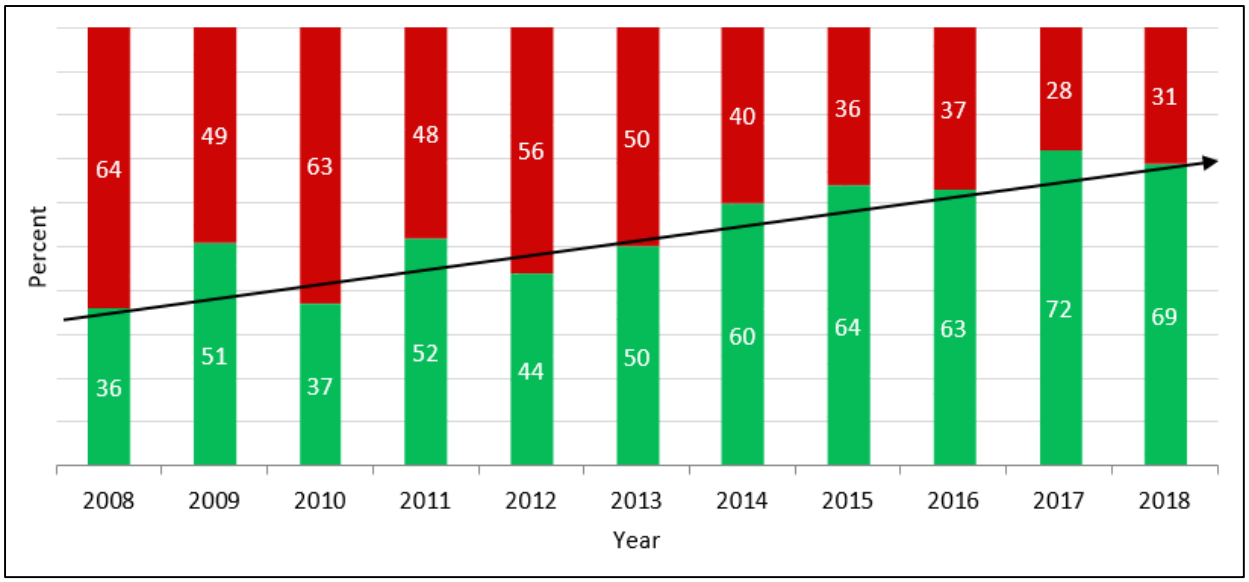
Weaknesses we found included:

- no BCPs or DRPs
- tolerable outages for critical systems not defined
- old and redundant DRPs with some not reflecting current ICT infrastructure
- DRPs never tested and entities not knowing 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 is essential to the effective and timely restoration of systems supporting entity operations and business functions.

Management of IT risks

Sixty-nine percent of entities met our expectations for managing IT risks, a 33% improvement since our first assessment in 2008. Entities showed improved management controls over IT risks.



Source: OAG

Figure 7: Management of IT risks

Weaknesses we found included:

- 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 entities 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 entities 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. This increases the likelihood that entity objectives will not be met.

IT operations

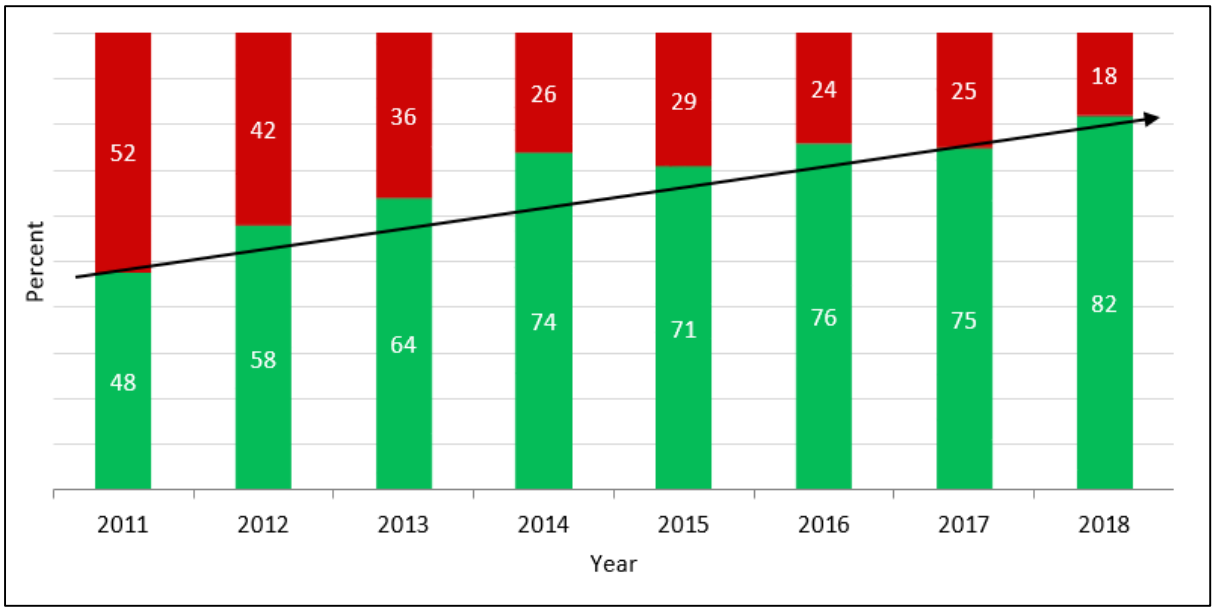
Entities' IT practices and service level performance to meet their business needs increased 7% compared to the previous year. There has been a steady improvement since 2011 when we first added this area to the CMM.

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

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

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

- effective preventative and monitoring controls and processes had 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:

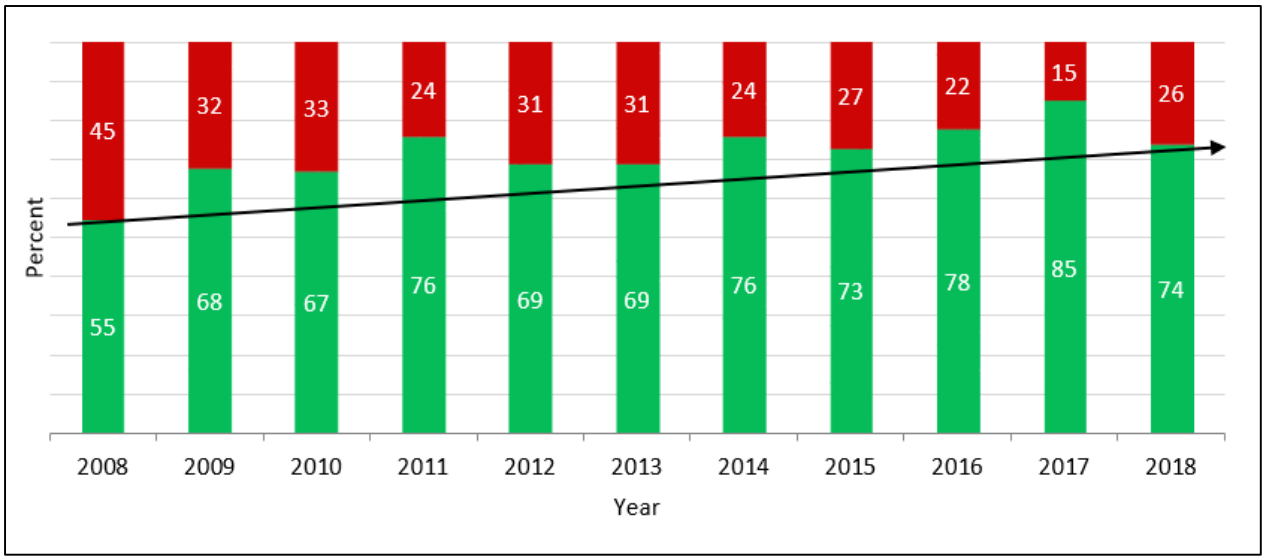
- information and communication technology strategies not in place
- lack of segregation of duties across finance, payroll and network systems
- no logging of user access and activity and no reviews of security logs for critical systems
- former staff with access to entity networks and applications after termination
- lack of policies and procedures and weak governance over ICT operations
- asset registers not maintained and ICT equipment unable to be located.

These types of findings can mean that ICT service delivery 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.

Although we saw a 9% decrease in performance in this category, change control practices have slowly been improving since 2008, with over 70% of entities achieving a level 3 or higher rating.



Source: OAG

Figure 9: Change control

Weaknesses we found included:

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

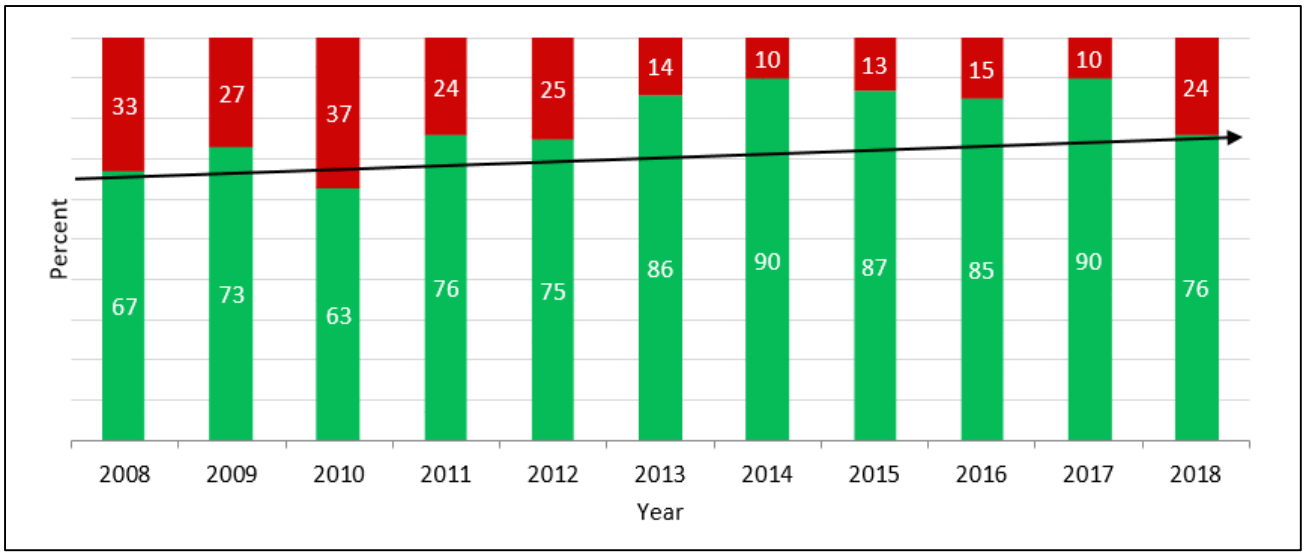
An overarching change control framework is essential to ensuring a uniform change control process and reliability of changes, and to improving performance through reduced time and staff impact. When examining change control, we expect defined procedures to be used consistently for changes to IT systems. 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 entities' 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 reviewed whether physical access restrictions were implemented and administered to ensure that only authorised individuals had the ability to access or use computer systems.

Seventy-six per cent of entities met our expectations for the management of physical security. However, this represents a 14% decrease from 2017 in the number of entities that met our expectations for physical security.



Source: OAG

Figure 10: Physical security

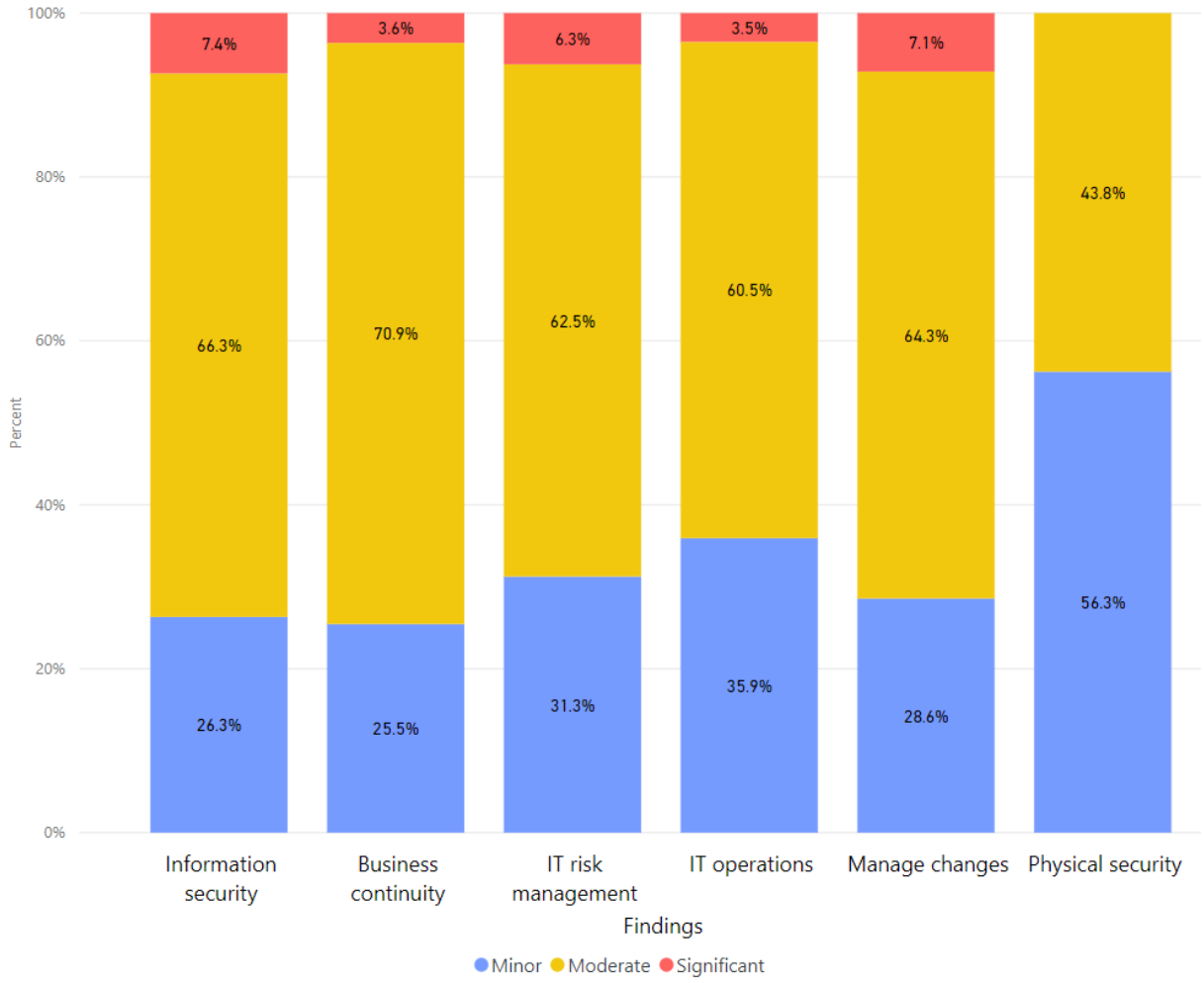
Weaknesses we found included:

- no reviews of staff and contactors' access to computer rooms
- backup power generators not tested
- lack of humidity controls in server room
- 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 summarises how we rated the significance of our findings. It shows that the majority of our findings were 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, combinations of issues can leave entities with more serious exposures to risk.



Source: OAG

Figure 11: Distribution of ratings for GCC findings in each control category we reviewed

Recommendations

1. **Information security**

   Executive managers should:

   a) ensure good security practices are implemented, up-to-date, regularly tested, and enforced for key computer systems
   b) conduct ongoing reviews of user access to systems to ensure they are appropriate at all times
   c) develop and implement mechanisms to continually raise information and cyber security awareness and hygiene among staff at all levels.

2. **Business continuity**

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

3. **Management of IT risks**

   Entities 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.

4. **IT operations**

   Entities 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 entities' strategies and objectives. The OAG recommends the use of standards and frameworks as references to assist entities with implementing good practices.

5. **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 occurrence of problems. Change control documentation should be current, and approved changes formally tracked.

6. **Physical security**

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

Appendix 1 – Cloud application (SaaS) better practice principles

In a software as a service (SaaS) arrangement, responsibility for cyber security is shared between the vendor and customer. Public sector entities remain responsible for security including governance and access to information. Entities should assess the risks associated with handing over data to vendors and ensure sufficient controls are in place to meet each entity's security needs, including that contracts include measures to mitigate risks and protect information held in the cloud. Ongoing contract management is also essential and should include the entity verifying that the vendor adheres to agreed terms. This may occur through third party assurance reports and entity reviews.

The following table shows some better practice principles entities should consider when choosing a SaaS provider and considerations for ongoing contract management. This is not intended as an exhaustive list. Further guidance can be obtained from the Australian Cyber Security Centre[4].

Stage	Principle	Our expectation
Decision to adopt SaaS	Understand risks	Perform a risk assessment to understand security risks associated with handing over information to a cloud vendor. The sensitivity, use and value of data should inform an understating of the risks to be closely managed when weighing value for money considerations
	Vendor	Knowing who the vendor is and what they do. Vendor reputation and its compliance with recognised security standards should be assessed. The Australian Cyber Security Centre maintains a list[5] (CCSL) of Australian government certified cloud vendors
SaaS contract and management	Security	Appropriate controls should be defined to protect the application and existing ICT systems that interact with the application from cyber attacks
	Data sovereignty	Data is subject to the laws of the country where it is stored. Entities should prefer an arrangement where data is stored in Australia. If this is not possible, the nature of data going overseas and laws of those countries should be carefully considered
	Data ownership	Contracts should clearly state who has legal ownership of any data during and after the contract
	Data retention and deletion	Contracts should clearly define the data retention method and period
	Access to data and monitoring	Controls to restrict and monitor access to data should be in place
	Vendor lock-in	Controls to enable efficient migration of data to other cloud or on premise systems, should be defined. An exit strategy should be agreed with the vendor to support the move

[4] https://www.cyber.gov.au/publications/cloud-computing-security-considerations

[5] https://acsc.gov.au/infosec/irap/certified_clouds.htm

	Encryption of data	Appropriate levels of encryption should be defined for data in transit and at rest. This should also include management of the data encryption key
	Data segregation	Many SaaS applications provide access to multiple customers on a shared platform. Controls should be in place to segregate data from other tenants
	Security breaches	Contracts should clearly define how the vendor must report security breaches and include penalties and indemnities. Entities should have access to relevant evidence (e.g. logs) for forensic investigations
	Availability of application and data	Data backup requirements should be defined and vendor disaster and business continuity plans should meet the entity's business needs. Contracts should define acceptable down times and penalties. An appropriate escrow agreement should be considered if the SaaS application is built or highly customised for the entity
	Strong authentication controls	Access to cloud applications and data should have strong controls and include multifactor authentication
	Assurance reports	Vendors should provide independent audit assurance reports (e.g. SOC 2) to confirm vendor controls meet expectations and operate effectively
	Right to audit	Contracts should define the entity's right to conduct a security audit of vendor controls to protect the confidentiality, integrity and availability of applications and information
	Background checks	Vendors should perform background and criminal history checks for their staff. Security clearances should be considered for highly sensitive data
	Ongoing contract management	Vendor compliance with agreed terms should be regularly checked.

Auditor General's Reports

Report number	Reports	Date tabled
19	Audit Results Report – Annual 2018 Financial Audits	15 May 2019
18	Firearm Controls	15 May 2019
17	Records Management in Local Government	9 April 2019
16	Management of Supplier Master Files	7 March 2019
15	Audit Results Report Annual 2017-18 Financial Audits of Local Government Entities	7 March 2019
14	Opinions on Ministerial Notifications	13 February 2019
13	Opinion on Ministerial Notification	23 January 2019
12	Managing Disruptive Behaviour in Public Housing	20 December 2018
11	Opinions on Ministerial Notifications	20 December 2018
10	Opinions on Ministerial Notifications	18 December 2018
9	Treatment Services for People with Methamphetamine Dependence	18 December 2018
8	Opinions on Ministerial Notifications	10 December 2018
7	Audit Results Report – Annual 2017-18 Financial Audits of State Government Entities	8 November 2018
6	Opinion on Ministerial Notification	31 October 2018
5	Local Government Procurement	11 October 2018
4	Opinions on Ministerial Notifications	30 August 2018
3	Implementation of the GovNext-ICT Program	30 August 2018
2	Young People Leaving Care	22 August 2018
1	Information Systems Audit Report 2018	21 August 2018

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