Western Australian
Auditor General's Report

Information Systems Audit Report

Report 12: June 2017

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

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Information Systems Audit Report

Report 12
June 2017

WESTERN AUSTRALIA

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

INFORMATION SYSTEMS AUDIT REPORT

This report has been prepared for submission to Parliament under the provisions of sections 24 and 25 of the *Auditor General Act 200*6.

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.

COLIN MURPHY
AUDITOR GENERAL
29 June 2017

Contents

Auditor General's Overview

This is my ninth annual *Information Systems Audit Report.* The report summarises the results of the 2016 annual cycle of audits, plus 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.

Disappointingly, I must again report that many agencies are simply not taking the risks to their information systems seriously. I continue to report the same common weaknesses year after year and yet many agencies are still not taking action. This is particularly frustrating given that many of the issues I have raised can be easily addressed. These include poor password management and ensuring processes to recover data and operations in the event of an incident are kept updated.

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. As recent high profile malware threats have shown us, no agency or system is immune from these evolving and ongoing threats. The risk to agency operations and information is real and needs to be taken seriously.

Our applications reviews show that agencies also need to take the initiative and perform their own business process 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 risks and make improvements.

I must stress that this report is not all bad news. In the first part of this report, I identified some good practice and improvements across 5 key business applications. And in the second part of this report, I was pleased to identify 3 agencies that have consistently demonstrated good management controls.

It has not been my practice to name agencies when weaknesses are found in their general computer control environment as this could potentially expose these agencies to hackers. By naming those agencies that have demonstrated good practice and including case studies that show how agencies' security had been compromised, I hope to encourage improvement across the sector.

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. **Image and Infringement Processing System (IIPS)** – Western Australian Police
2. **Navigate** – Department of Racing, Gaming and Liquor
3. **Laboratory Information Management Systems (LIS)** – Chemistry Centre
4. **Case Management and Intelligence System (CMIS)** – Corruption and Crime Commission
5. **Project and Contract Management (PACMAN)** – Department of Finance

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.

Summary

All 5 applications had control weaknesses with most related to poor information security, policies and procedures. We also found issues with controls that aim to ensure the applications function efficiently, effectively and remain available. We reported 65 findings across the 5 applications with 4 of these rated as significant, 53 moderate and 8 being 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.

Key findings

Image and Infringement Processing System (IIPS) – Western Australian Police (WA Police), page 10

- WA Police shares sensitive information with third parties by transferring it in clear text across the internet. It also stores sensitive information unencrypted on back up tapes. Encrypting this information would help protect it from unauthorised use.
- WA Police relied on its contractors to patch systems but we identified known weaknesses not patched, thereby exposing systems to cyber threats and inappropriate access and misuse.
- User access was not appropriately controlled and privileged accounts not suitably managed. This exposes the application and its data to unauthorised access.
- Officers spend a substantial amount of time processing and fixing errors associated with on the spot fines. WA Police could automate processes to free up police resources.

Navigate – Department of Racing, Gaming and Liquor (DRGL), page 14

- Inadequate implementation of IT policies has led to password and user access controls that fall well below good practice. We were able to access sensitive documents in one of DRGL's systems without a username or password and we were able to create an account that allowed us to access confidential information. Credit card information was among the sensitive data at risk from these poor security controls.
- DRGL lacks continuity or disaster recovery plans and has not assessed the impact of an outage or disruption to its licensing system. As a result, a disruption could lead to significant delays with issuing liquor licences and could affect other agencies that rely on the system.
- Navigate requires a substantial amount of manual processing making it inefficient and puts the integrity of information at risk.

Laboratory Information Management Systems (LIS) – Chemistry Centre (ChemCentre), page 20

- Poor password security meant we were able to guess a large number of ChemCentre's passwords and thereby access highly privileged administrator accounts. A lack of patching to fix known security vulnerabilities also exposed ChemCentre's information and systems to breaches or misuse via a cyber attack.
- ChemCentre stores sensitive documents on the network providing all network users access to the information. Unencrypted backups are also provided to a third party for off-site storage. This creates a risk of unauthorised disclosure of information.
- ChemCentre has not assessed the impact of losing its applications and is exposed to significant data loss in the event of a major incident. Although ChemCentre has an alternative facility, it has not acquired the equipment to run the second site.

- Technology risks are not considered in ChemCentre's risk management framework, which can affect its strategic and operational requirements.

Case Management and Intelligence System (CMIS) – Corruption and Crime Commission (CCC), page 25

- CMIS has not had a risk assessment and the IT risk register has not been updated for 6 years. CCC's own policy requires a review of risks at least annually to ensure that it is fully aware of its risks. It has also not developed a disaster recovery plan for CMIS or other key systems and does not have a continuity agreement in place with its service provider.
- We identified out of date, unpatched software vulnerabilities on the servers that run CMIS as well as other key systems. Patches were missing as a result of an automated patching system that was not configured correctly.

Project and Contract Management (PACMAN) – Department of Finance, page 30

- The Department has not fully utilised PACMAN to alert it of potential payment delays and to store vital contract documentation. In 2015-16, the Department made a number of late payments to contractors to the value of over $13.3 million. We also found 1 project valued at over $28 million with no business case, project definition or project plan and another project valued at over $43 million with no procurement options detailed.
- Inconsistent monitoring of costs lead to under-billing of projects. From a sample of 20 projects, we noted 30% were under-billed. From the same sample, we found 15 projects were marked as completed up to 6 years ago but not finalised in PACMAN or the Finance system.
- The Department has not undertaken any testing of its disaster recovery plan. Without periodic testing of its plan, the Department cannot be confident that it can maintain the security, integrity and continuity of its systems in the event of a disaster or period of extended outage.

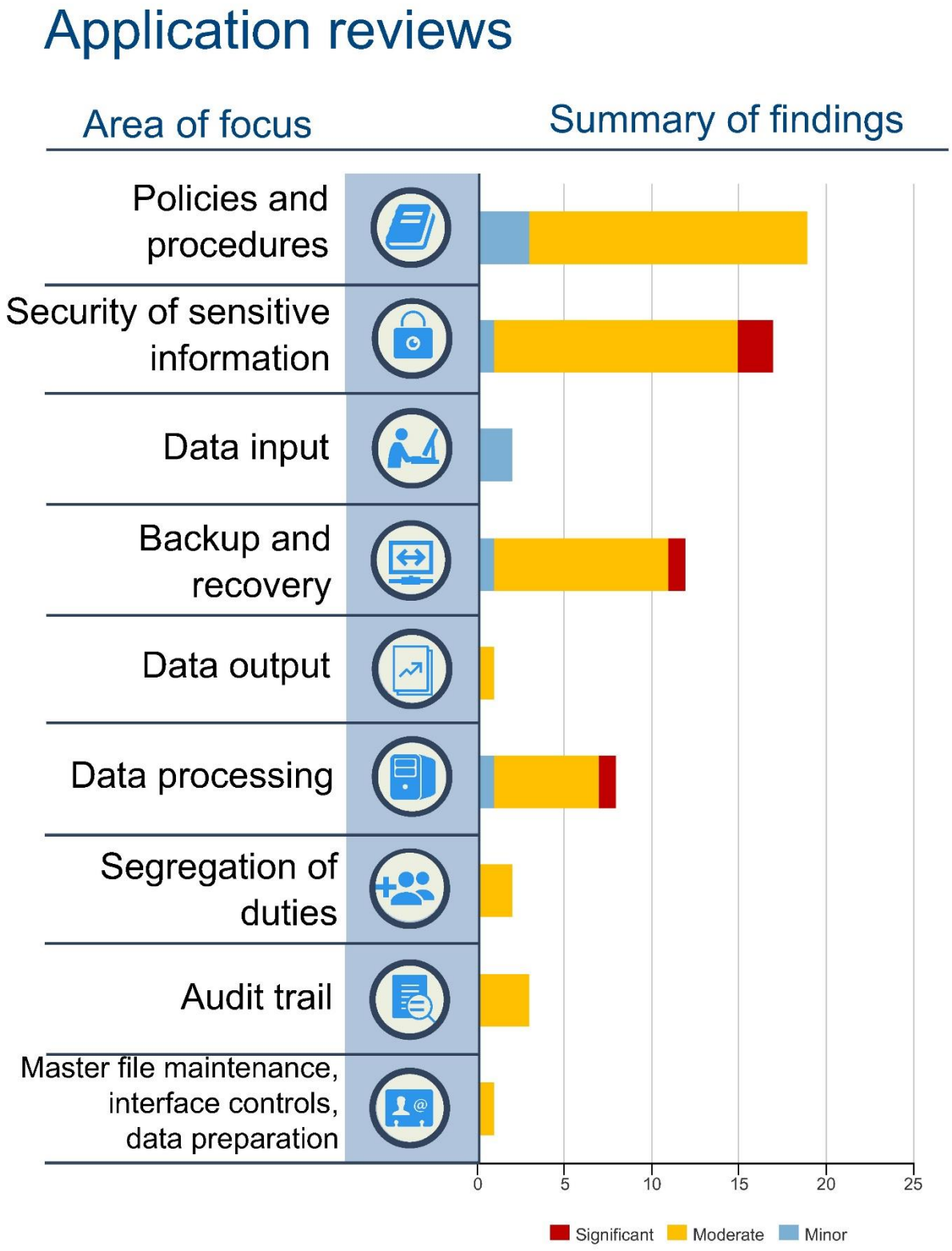


Figure 1: Application reviews

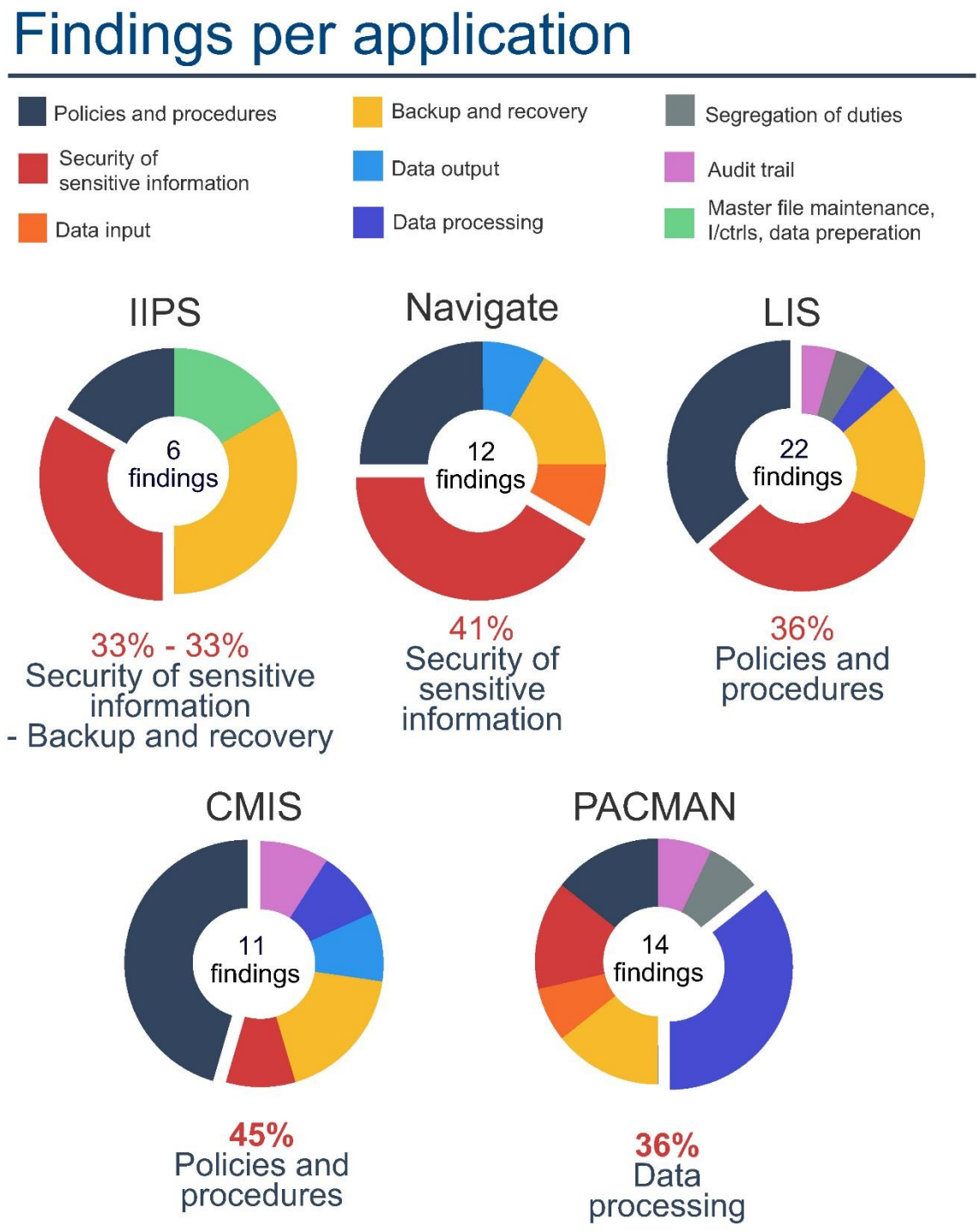
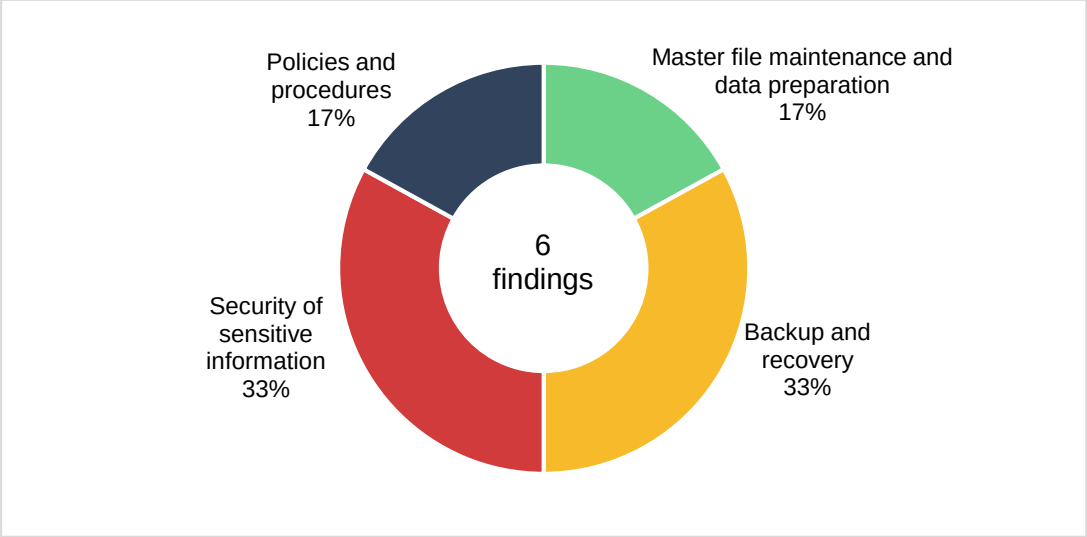


Figure 2: The areas of findings per application

Image and Infringement Processing System (IIPS) – Western Australian Police



Introduction

WA Police uses IIPS to manage traffic infringements caught by cameras and those issued by officers. The system stores confidential infringement data containing names, addresses and offence information.

Audit conclusion

WA Police can rely on this system to manage its traffic infringement processes effectively. However, there are some areas of weakness associated with the system.

A heavy reliance on manual paper-based processes associated with on-the-spot infringements has compromised the efficiency and integrity of the system. Police officers also spend considerable time managing and correcting data errors.

Information sharing arrangements with third parties is not secure, potentially increasing the risk of unauthorised access to confidential information. Poor management of user access rights and a significant number of software vulnerabilities further increase the risk of exposure of sensitive information or a cyber incident.

WA Police also needs to improve disaster recovery processes for IIPS. Not ensuring that its plans are adequate and up to date risks downtime and potential data loss.

Background

The Traffic Services Branch of WA Police has an important role to play in safeguarding and improving road safety in Western Australia. The branch manages the fleet of mobile speed cameras and fixed red light and speed cameras.

Within Traffic Services, the Infringement Management and Operations office is responsible for processing traffic infringements and overseeing camera operations.

In 2015, WA Police used IIPS to record and manage approximately 747,000 speeding infringements, 18,000 red light and 135,000 on the spot infringements. The Operations office, in conjunction with a third party vendor, developed IIPS in-house to suit its requirements.

Traffic incidents recorded by cameras (both mobile and fixed) are loaded into IIPS for processing. IIPS automatically converts these incidents into infringements, which different teams within WA Police verify prior to the system sending them onto traffic offenders.

Police officers also issue on-the-spot fines to offenders, and manually enter them into IIPS for processing.

Audit findings

Sensitive data is exposed and better protective measures should be applied

WA Police shares infringement data, containing names, addresses and offence information, electronically with a third party vendor in an insecure manner. This vendor prints and mails infringement notices to offenders using information provided to them over the internet in plain-text via a simple file transfer method. This increases the risk of a hacker intercepting sensitive information. WA Police is in the process of evaluating secure file transfers to see if it could use this solution to improve information security.

Sensitive and personal information from IIPS and other WA Police systems that is stored on backup tapes is also not appropriately secure. A third party collects and manages the tapes in off-site storage. If a tape was lost or stolen, an unauthorised party could read the information stored on the tape. WA Police needs to address this risk, for example by encrypting information to ensure that only people with appropriate authorisation can read it.

We tested a sample of 75 IIPS accounts, which showed that accounts for 3 former employees were still open and 2 other accounts did not appear on the access register.

Without appropriate controls covering user access, there is an increased risk of unauthorised or inappropriate access to sensitive information.

Considerable time is spent managing paper based infringements

On average, police officers issue about 11,500 ‘on the spot’ infringements to motorists each month. This type of infringement requires manual recording of the details of the driver, vehicle, and infringement, handwritten on paper tickets. Officers around the state must send hard copy tickets to the Operations office team for processing. The hard copies are scanned into IIPS for safekeeping and a team of dedicated data entry officers then enter the details of the tickets into IIPS.

These infringements may need to be cancelled or withdrawn if they contain:

- incorrect offence codes
- incorrect address information
- incorrect penalty amounts and/or demerits.

We checked a sample of 50 cancelled on the spot infringements, and found that half of these were withdrawn due to incorrect details. Although the infringements are usually reissued with the correct details, officers spend considerable time processing the cancellation and fixing the errors.

Opportunity exists for WA Police to automate on the spot fines to reduce its reliance on handwritten tickets. This automation could reduce the risk of errors, and free up police resources for other duties.

Security vulnerabilities may go undetected due to inadequate processes

We found software updates released by vendors to fix known security issues were not applied to the system, including 162 'critical' and 'high' severity updates. We also identified a number of serious vulnerabilities in software installed on the IIPS servers. Given the nature of the WA Police network, this is a serious concern.

WA Police relies on its contractor to identify vulnerabilities. However, the tools used for the assessment are not configured correctly to be fully effective, meaning that vulnerabilities may go unpatched. Currently, there are dozens of ways for hackers to exploit the vulnerabilities and compromise the system. An effective vulnerability management process is essential in order to mitigate against these cyber threats.

Disaster recovery plans have not been tested and may be unreliable

WA Police does not have adequate procedures and plans to recover IIPS in a disaster situation. Although plans and backup equipment are in place, there has been no testing of the disaster recovery process. Without this testing, WA Police cannot be sure that its plans are effective. IIPS is a critical system and an outage would result in delays to infringement management operations. Regular testing of recovery procedures is important to highlight gaps and to better prepare WA Police for a disaster situation.

Recommendations

1. **By December 2017, WA Police should:**
    a. **review the information security policy to ensure appropriate controls are in place to protect sensitive information**
    b. **review the process for managing security vulnerabilities, software updates and patches**
    c. **review its manual processes for on the spot infringements and consider automated solutions**
    d. **develop access management policies and controls for the system**
    e. **develop and test disaster recovery procedures to ensure the timely recovery of systems following an incident or outage.**

Response from WA Police

WA Police fully accepts all of the Office of the Auditor General's recommendations and provide the following comments.

Recommendation (a) ensure appropriate controls in place to protect sensitive information

Police are in the process of implementing secure file transfer protocols with the print provider which is scheduled for completion in August 2017.

Recommendation (b) review practices for managing security vulnerabilities, software updates and patches

Police are currently upgrading to supported hardware and software components that will allow IIPS to be aligned with broader systems patch and vulnerability management.

Recommendation (c) consider automated solution to replace handwritten infringements

Police support the move to automated infringement solutions for frontline officers and intend to investigate potential solutions including linkage to a mobility platform.

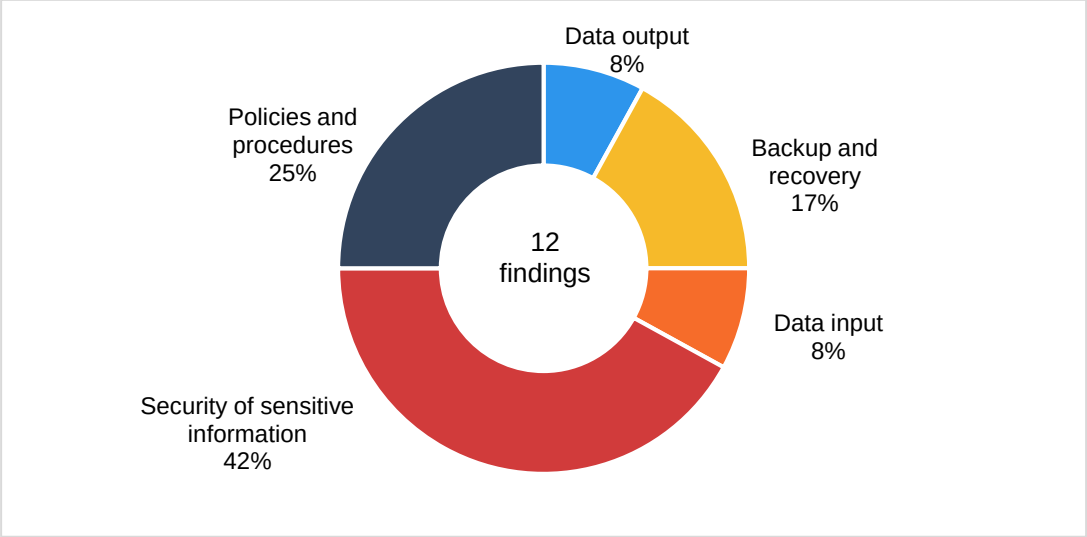
Recommendation (d) develop access management policies and controls

Access management practices have been reviewed and hardened until additional automated controls become available.

Recommendation (e) test DR procedures to ensure timely recovery

Disaster recovery documentation is currently being updated and will include the required test plans.

Navigate – Department of Racing, Gaming and Liquor



Introduction

The Department of Racing, Gaming and Liquor (DRGL) uses Navigate to manage gambling and liquor licensing and inspections. This system contains sensitive information such as proof of identity of applicants for a licence, the qualifications of applicants and criminal history and probity checks.

Audit conclusion

Navigate largely achieves its purpose, allowing DRGL to manage licensing, compliance and returns. However, the system has various weaknesses that affect its efficiency and pose a risk to its reliability and security.

Inadequate scoping of the system specifications has resulted in the use of substantial and inefficient manual workarounds to achieve its purposes. Security vulnerabilities also potentially expose personal information to hackers. Business continuity and IT disaster recovery plans are not in place to minimise the impact on operations and potential data loss in the event of a serious incident or disaster. Such plans are fundamental good practice.

Background

DRGL regulates the racing, gambling and liquor industry in Western Australia. It is responsible for licensing and compliance services for the racing, gaming and liquor industries.

There are over 80 different types of licence applications across liquor and gambling, including permits required to work at a casino. Every year, on average, DRGL processes approximately 12,000 liquor licences, 2,200 gaming permits and 1,000 licences related to bookmakers and casino employees.

DRGL conducts approximately 7,500 inspections, audits and assessments every year as part of compliance activities across the liquor, gaming and racing industries.

Applicants for a licence need to supply personal information that can include proof of identity, qualifications and criminal history and/or probity checks. DRGL scans and stores these documents electronically.

To improve its management of licensing, compliance and gaming returns, DRGL selected Navigate; a commercial off-the-shelf system to replace 3 legacy systems. DRGL started using Navigate in March 2015.

DRGL collects information from applicants and clients using paper-based and some online forms. The paper-based forms are checked for completeness and are then entered into Navigate. Due to the manual effort this requires, DRGL has a project underway to bring all applications online.

Audit findings

Security vulnerabilities are not managed to protect private data

DRGL did not conduct vulnerability assessments before deploying the Navigate system, which includes the public website, Navigate Portal. The public uses this website to lodge licence applications and upload compliance documents.

Vulnerability assessments are an important tool for securing systems. Servers and applications are searched for missing software patches or updates and insecure configurations. These assessments are crucial for any system that is available to the public via the internet. An attacker could use exposed vulnerabilities to gain unauthorised access to the online system, and possibly DRGL's internal network. This would then allow them to attack internal systems and access sensitive data.

Although DRGL has a process for installing software updates, we nevertheless found vulnerabilities in a number of its systems, including Navigate and its underlying database.

What can happen when software updates are not applied in a timely fashion?

During our testing, we found a serious security vulnerability in one of DRGL's systems due to missing software updates. This system was accessible from the internet and whilst not part of Navigate, DRGL used it as a file sharing portal to store licensing documentation.

Taking advantage of the vulnerability we had identified, we were able to access sensitive documents without needing a username or password. We were also able to create a highly privileged account (system admin), that gave us unrestricted access to all Navigate information and other user accounts.

The security of electronic records needs improvement

Navigate stores personal information on licence holders, much of which is confidential. Improvements are needed to the security of this information.

Some of the weaknesses we noted were:

Credit card information may be at risk. Hard copy and online licence applications contain credit card information for payment of fees. While DRGL generally has good practices to handle credit card data, we found a gap where unprotected/unmasked card details are retained for long-term storage on backup tapes. Processing and storing credit card information without appropriate levels of protection significantly increases the risk to DRGL and the individuals concerned. This is also in breach of Payment Card Industry Data Storage Standards. Unprotected credit card information may be misused or compromised.

Database passwords were easily guessed. We identified high privilege (sys and system) database accounts with very easy to guess passwords. Examples include passwords such as 'abcd' and passwords only one character in length. We also found that:

- password aging was not enforced including an unrestricted administrator account password which was not changed for over a year

- a large number of inactive system accounts had not had their default passwords changed.

Password security is fundamental good practice, which if not enforced could lead to unauthorised access.

Backups not encrypted. Unencrypted backups are stored on tapes for collection and management by a third party contractor. This creates a risk of unauthorised access and inappropriate disclosure of information if stored tapes are misused or lost or stolen. Encryption ensures that the data cannot be accessed without the decryption keys. Encryption of backup media where confidentiality is important is in accordance with the international standard for information security (ISO27002/2013).

IT processes to support Navigate are incomplete or not in place

Deficiencies in DRGL's IT policies, risk management, business continuity and IT planning have resulted in a range of weaknesses in application, database and network security controls. This places the security of sensitive information at risk.

User permissions are not reviewed. There are no processes to review the appropriateness of user permissions within the Navigate system. When users act in higher roles or move between different divisions (e.g. licensing, compliance), their access authority is changed to suit the new role. However, the application cannot enforce an 'end-date' or expiry for temporarily assigned privileges meaning that the revoking of prior permissions may not occur in a timely manner.

External accounts are not well managed. DRGL has good access control policies and procedures covering network user accounts. However this does not include regular reviews of external accounts. These external users from other WA government agencies access Navigate information via a reporting tool. We found 15 unused (never logged in) accounts that were created over 12 months ago and 16 accounts not used in over 9 months. Without appropriate controls and formal procedures covering user access reviews, there is an increased risk of unauthorised or inappropriate access.

There is no high level review of changes. A suitable governance arrangement that includes relevant stakeholders is not in place to review and approve new enhancements, customisations and fixes to Navigate. A process is required to ensure that the impact of any significant changes is considered at a whole of department level. Changes also need to be consistent with the strategic direction of DRGL.

Change procedures are not followed. DRGL has well documented procedures that explain the process to make changes to IT systems, including Navigate. However, records of system changes are not stored in a centralised register, despite this being a requirement of the configuration procedures. Inadequate configuration and change management increases the risk that proposed changes to Navigate are not well described and assessed and/or implemented correctly.

There are no disaster recovery plans

DRGL has not assessed the impact of an outage or disruption to the Navigate system, and developed business continuity or IT disaster recovery plans for this situation. Significant delays to the issuing of licences and to DRGL's compliance activities would occur if Navigate was not recovered within acceptable timeframes. An outage would also affect other government agencies that rely on Navigate.

In the event of a disaster, a business continuity plan helps ensure that critical departmental services can be provided, usually with manual processes and other temporary workarounds. A disaster recovery plan provides details of the procedures to follow to recover the system in the event of an incident or disruption.

DRGL also does not have arrangements in place to recover systems from a secondary site should the primary location be affected by a serious event.

The capacity to restore Navigate in a timely manner is made harder by undocumented changes made to Navigate. We found a variety of ad hoc and undocumented changes. Some of these are temporary workarounds while a fix or system enhancement is developed. While DRGL has documentation that covers the initial building and deployment of Navigate, the subsequent changes are not included. In the event of a disaster, this could mean that the workarounds are not restored properly, affecting Navigate's functionality and licensing processes.

Navigate requires manual workarounds and does not fully support DRGL's needs

Navigate is a system that requires substantial manual processes and workarounds to complete important tasks, despite it being a relatively new system – just 2 years old. When establishing why this was the case, we found that the system's development was problematic – being 11 months late and 44% ($2.1 million) over budget. It was also evident that the system requirements were not well considered, resulting in significant inefficiencies.

Efficiency measures such as automated workflows were not fully incorporated into the new system and as a result, a substantial amount of manual processing is required to collate and link information in the system. Manual workflows are inefficient and increase the risk of inaccurate and/or incomplete information.

Examples include:

- There is no function to update documents directly in the Navigate system. Users are required to download documents to a temporary place, edit them, and then re-upload them.
- Licensing officers do not receive automatic notifications when an objection to a proposed liquor or gaming licence is lodged. Objections to a licence application are stored on shared network drives. Licensing officers need to perform manual searches to identify any new objections, and to determine if they are relevant to a licence application.
- To create new licence applications or initiate compliance investigations, officers manually select clients from a database and link them to premises and other key information. Officers are required to search for the same information multiple times to complete mandatory, duplicated fields.

Lack of validation controls increase the risk that data is inaccurate

We found that Navigate does not enforce validation on all entered data. The system accepts duplicate entries, invalid information and incorrect dates such as a date of birth that is in the future.

Hard copy licence applications are entered into the system manually. DRGL has a project underway to bring all applications online, which will reduce the extent of manual data entry. This is a good initiative to improve data collection efficiency.

Lack of validation controls increase the risk of inaccurate, duplicate and/or incomplete information affecting the quality of data.

Recommendations

1. **By December 2017, the Department of Racing, Gaming and Liquor should:**
    a. **review any manual processes and consider if it can automate them**
    b. **conduct business impact assessments and develop a disaster recovery plan for its key applications and services to ensure the timely recovery of systems following an incident or outage**
    c. **review its management of security vulnerabilities and conduct regular vulnerability assessments**
    d. **review the information security policy to ensure**
        - **access management for systems is defined**
        - **appropriate controls are in place to protect sensitive information**
        - **database account passwords follow good practice for access management and comply with internal policy requirements**
    e. **establish appropriate controls to ensure accurate data entry and validation**
    f. **establish a suitable governance arrangement to oversee significant changes to Navigate and to ensure that configuration processes are followed in line with good practices and internal policy**
    g. **ensure that in procurement processes, limitations are not placed on technology solutions that limit strategic options or result in long-term contracts with single suppliers.**

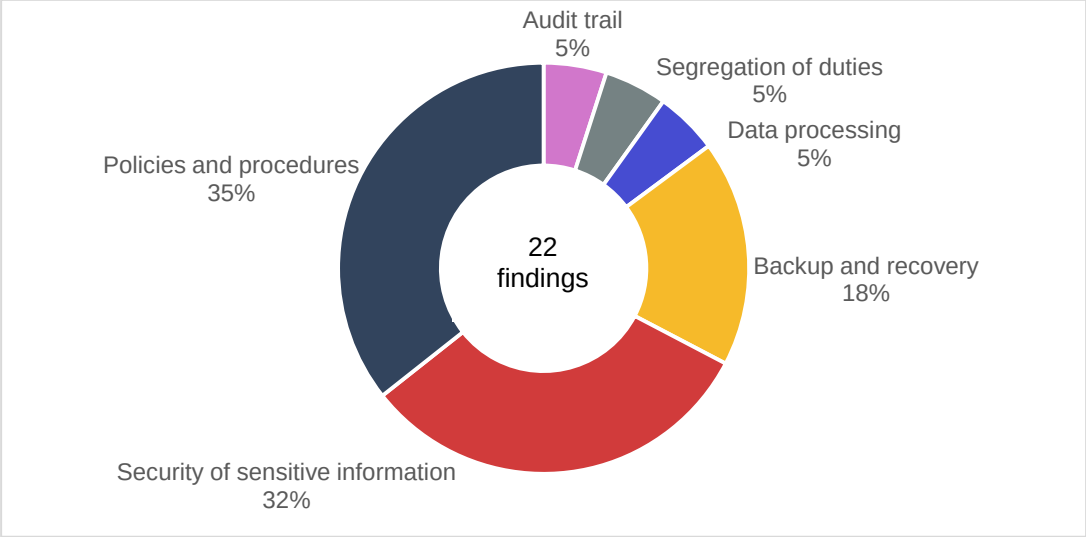
Response from the Department of Racing, Gaming and Liquor

The department accepts fully all recommendations and has responded to the summary of findings from the audit. Action already taken addresses all the recommendations. These actions include:

- Continuing with a project to make all applications available online, reducing manual data entry and enforcing validation controls. This initiative requires an update to current portal technology with a planned implementation in October 2017;
- Conducting comprehensive business impact assessments and developing disaster recovery plans for all business systems;
- Undergoing system vulnerability and penetration testing for Navigate and associated portals and addressing identified system weaknesses;
- Updating all relevant information security policies and practice;
- Implementing a process of quality control to ensure data accuracy and validation; and
- Implementing an appropriate internal governance structure to oversee changes to Navigate, portal and other information systems.

In March 2017, consultants were engaged by the department to conduct a review of responses to the findings and recommendations made by the Office of the Auditor General following their audit of the Navigate system. The consultants' review also assessed the response to the findings raised within the penetration and vulnerability test that was performed in December 2016 to February 2017. All findings from that review have also been addressed.

Laboratory Information Management Systems – Chemistry Centre



Introduction

ForLIMS and SIGNA are the two laboratory information management systems used by the Chemistry Centre (ChemCentre) to manage laboratory operations. These systems contain highly confidential information and if not managed properly could compromise the reliability and accuracy of important laboratory results.

Audit conclusion

ForLIMS and SIGNA allow ChemCentre to manage the operations of its laboratories and helps ensure the integrity of its analysis and reporting.

However, system integrity is at risk from a range of weaknesses in application, database and network security controls. These include weak passwords, unpatched software and inadequate access controls and disaster recovery plans.

Background

ChemCentre provides analytical services to government agencies and industry for forensic science and medicine, public health and safety, environmental protection, and crisis and emergency response and management.

It delivers these services through two independent laboratories: the Forensic Science Laboratory (FSL) and the Scientific Services Division (SSD). Each laboratory manages its operations through bespoke Laboratory Information Management Systems.

The FSL provides forensic services to WA Police, state and district coroners, and other government agencies. Analysis results reported by FSL are sensitive in nature and confidential until released to the public by the relevant agency. Inaccurate reporting could result in misreporting of results to clients.

ChemCentre created ForLIMS in the early 1990s specifically to meet FSL's needs for managing and reporting of forensic cases. FSL has continually updated ForLIMS and it now contains over 130,000 cases. In the year to June 2016, FSL processed over 9,500 cases and tested almost 58,000 samples.

ChemCentre's other laboratory, the SSD, provides a wide range of scientific services to government and industry clients including emergency response to chemical incidents. Its

stated aim is to safeguard the state from chemical risks to health and safety and facilitate sustainable economic development. Its services including testing of soil, water, air, and other materials for harmful chemicals.

SIGNA is a major in-house redevelopment of a legacy laboratory application, which SSD uses to manage laboratory operations. In the 12 months to June 2016, SSD performed over 510,000 tests on approximately 2,600 jobs for over 500 clients.

Audit findings

Poor policies and procedures compromise data security

ChemCentre lacks many of the information security policies and procedures needed to ensure the security of applications. The policies that do exist are outdated and may no longer be suitable. Policies and procedures set senior management expectation and responsibilities for configuration of security controls to meet security requirements. They also inform employees of their responsibilities for security.

ChemCentre applies many technical controls to ensure the security of its applications and information. However, many of these controls may not meet its security objectives, as the policies are lacking or outdated.

For example, the password policy, last reviewed in 2010, allows users to set simple passwords such as ‘password’ or ‘12345678’. In addition, the policy does not require stronger passwords for highly privileged network, database and application accounts. As a result, we were easily able to guess passwords for the database system administrator account and for accounts within ForLIMS.

ChemCentre does not have a policy for the logging and monitoring of key events in its applications. While key events in SIGNA and ForLIMS are recorded in ChemCentre’s IT systems, there is no requirement to proactively monitor or act on these. This means ChemCentre may not recognise or respond to attempts to compromise its applications or data until after the fact. We also noted that key database events are not recorded, such as access attempts, account administration and changes to database configuration.

Out of date and unpatched software leave applications exposed

We identified out of date and unpatched software on the server that runs ForLIMS and SIGNA as well as other core systems and workstations. In particular, the database software is an out of date unsupported version. These patches were missing because ChemCentre does not have a process to identify and act on vulnerabilities in its software. Without regular updates, attackers could exploit known vulnerabilities and may gain access to ChemCentre’s systems and data.

ChemCentre uses specialist scientific equipment to perform analysis on the samples it receives from clients. This specialist equipment is connected to ChemCentre’s network to allow the transfer of data with its applications. In addition, to allow monitoring of long running jobs ChemCentre enables remote access to some of the equipment.

Due to hardware and/or software limitations, much of the specialist equipment runs on legacy unsupported operating systems with known exploitable vulnerabilities. An attacker exploiting an unpatched workstation in ChemCentre’s corporate network may gain access to the specialist equipment rendering it inoperable. ChemCentre needs to use layered security controls such as network segmentation to make it as difficult as possible for attackers to gain access. The Australian Signals Directorate considers network segmentation to be an excellent control to limit cyber-attacks.

Sensitive data is at risk of unauthorised access

ForLIMS and SIGNA have access restrictions in place; however, these applications store electronic documents on the network, which is not subject to the same access controls. This may allow a user with network access to gain unauthorised access to the reports.

ChemCentre generates backup tapes of application data for future recovery, which a third party collects for off-site storage. These tapes are unencrypted, which creates the risk of unauthorised disclosure of information if they are lost or stolen. Encryption of backup media is advisable where confidentiality is important, as outlined in the international standard for information security (ISO27002/2013).

The work performed by ChemCentre may be sensitive particularly where the Forensic Services Lab is involved in ongoing investigations on behalf of the police or coroner.

Inadequate continuity planning increases risk of data loss and disruption

Government agencies and commercial entities depend on the results of timely and accurate analysis provided by ChemCentre. The ForLIMS and SIGNA applications allow ChemCentre to manage the volume and priority of jobs within the laboratories. While ChemCentre would be able to manage urgent cases through manual procedures, an outage to ForLIMS or SIGNA would likely result in delayed reporting to clients, reputational damage to ChemCentre and loss in clients.

ChemCentre has limited understanding of the potential impact of a disaster. In 2011, ChemCentre conducted some analysis on the potential impact of an extended outage of its applications. However, the scope was too limited and it has not revisited it since. Understanding this impact is essential; it allows ChemCentre to invest the right amount of money and effort into planning for system recovery, as well as the manual processes required to maintain operations during an outage.

Because of this limited analysis, ChemCentre's current disaster recovery plans are not sufficient to recover the applications. These plans should be written with enough detail so that any person with the right skill set can recover the systems if required. A high level of detail also ensures that during a high-pressure recovery event, recovery steps are not missed and are performed consistently and correctly.

Backup tapes are kept but are not well managed. A key component of the recovery effort will be restoration of data from backup tapes. We found that the tapes are not removed from the tape library for up to 5 days after a backup is taken, increasing the chance of both original and backup tapes being destroyed in the one disaster event. In addition, the tape library is located in the same room as the production servers so both would be destroyed if flooding or fire for example occurred in that room. These issues expose ChemCentre to significant data loss in the event of a major incident or disaster.

We also noted that while there is an alternative facility available to run essential systems, ChemCentre has not purchased key hardware and would need to rapidly acquire and install this equipment following a disaster.

ChemCentre has not properly assessed risks to its laboratory information systems

ChemCentre's current risk framework addresses the safety of its staff, but does not consider broader strategic and operational risks, including technology risks.

There is no guidance for the identification, assessment and treatment of technology risks, which can include information security incidents such as malware and unauthorised access or computer outages. As a result, the ICT team conducts technology risk assessments in isolation to business objectives and strategies. While the ICT team will have good technical knowledge of the applications, they are unlikely to understand fully the impact of risks to business objectives.

ChemCentre also does not review how effectively its controls are operating. It is important to conduct regular reviews of controls to be sure they continue to address identified risks within business requirements. In addition, ChemCentre does not record control and risk treatment information in its risk register. A risk register helps communicate risk within an organisation. Without this information, ChemCentre cannot be fully aware of its technology risk, exposing it to a range of potential security, integrity and access issues.

Lack of strategic planning means applications may not meet future requirements

ChemCentre invests significant money and resources in the continued development of ForLIMS and SIGNA. A lack of short and long term planning along with inadequate documentation may jeopardise the ability for these applications to meet the organisation's future needs.

ChemCentre has not properly planned for the long-term future of the applications. Strategic planning for applications is critical and should consider ChemCentre's corporate strategy as well as issues such as technology changes, the need for two laboratory systems and buy versus build. A lack of sufficient strategic, forward thinking has seen ForLIMS and SIGNA developed using unsupported environments, thereby increasing the risk to IT and business operations.

ForLIMS and SIGNA are bespoke applications, created and maintained in-house by ChemCentre's developers. This team is making continual enhancements to the systems to meet the changing needs of ChemCentre. However, ChemCentre does not have a formal software development process to ensure it is selecting the most suitable, cost-effective and timely enhancements.

ChemCentre does not have a change management procedure. This is necessary to ensure that it appropriately plans and approves changes to its applications. A key step in the development process is to test that the enhancement meets business requirements and does not introduce errors. ChemCentre has development and test environments in place. However, we found these to be on the same server as the production environment. In this configuration, development and/or testing activity could affect the production environment.

Recommendations

1. **By August 2017, ChemCentre should:**
    a. **develop new and review existing security policies**
    b. **update its risk management framework and conduct a risk assessment of ForLIMS and SIGNA. Update the risk register with the results of the assessment and develop treatment plans if required**
    c. **conduct a business impact assessment and develop a disaster recovery plan for its key applications and services**
    d. **review the process for managing software vulnerabilities, patches and updates**
    e. **develop an IT strategic plan, software development process and update application documentation**
    f. **ensure appropriate controls are in place to protect sensitive information.**

Response from ChemCentre

ChemCentre welcomed the performance review of application controls for the two Laboratory Information Management Systems (LIMS) in operation within the organisation; Signa and ForLIMS. As a small agency (118 FTE in 2016-17) with limited IT staff resources, ChemCentre is appreciative of the assistance by the Auditor General's office to improve its IT systems in this manner.

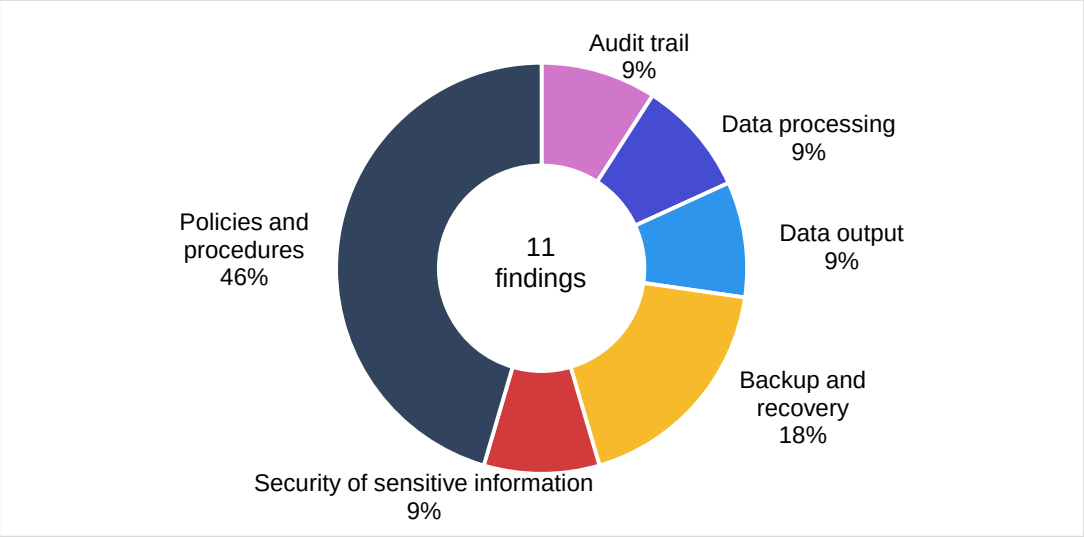
ChemCentre accepts fully the recommendations and has made significant progress to date in addressing each of the items raised. Issues with a higher risk designation ('significant or 'moderate') have been given due priority and all items rated 'significant' have been completed.

In May 2017 ChemCentre absorbed the operations of the Commonwealth National Measurement Institute's (NMI) Perth laboratory, along with 20 additional FTEs. This has required an exceptional investment in IT time and resources for the integration of new functionality into the existing Signa LIMS.

This one-off event has impacted the progress in addressing all the issues identified in the report.

Many of these remaining items will be addressed by the August deadline however, despite recruiting additional IT staff resources, it is anticipated that some items will not be completed until shortly after this date.

Case Management and Intelligence System (CMIS) – the Corruption and Crime Commission



Introduction

The Corruption and Crime Commission (CCC) uses CMIS to manage serious misconduct allegations and investigations. The system stores sensitive information about serious public sector misconduct allegations and investigations including case notes, logs, actions taken, and details of evidence. In 2015-16, the CCC used CMIS to log 2,244 notifications of serious misconduct, resulting in 4,024 allegations requiring assessment. Seventy-nine notifications resulted in an investigation by CCC.

Audit conclusion

CMIS supports the management and investigation of serious misconduct allegations for CCC. However, a number of weakness affect the security, reliability and efficiency of the system.

Poor risk management, missing security updates, poor IT processes and a lack of disaster recovery and continuity planning compromise the security of data and ongoing availability of information.

The rigid design of the system requires inefficient manual work-arounds and does not allow for interactive reporting, limiting its usefulness to CCC.

Background

CCC deals with allegations of serious misconduct by public officers in Western Australia. These include police, prison officers, teachers, public servants, local government and members of Parliament.

Serious misconduct can include fraud, stealing, tax evasion, excessive use of force, trafficking of drugs and deliberately releasing confidential information.

CCC is notified of serious misconduct, which can then lead to formal allegations. Allegations require thorough investigation by either CCC or the associated government agency.

CCC uses CMIS to manage the notifications and allegations they receive. If it decides to undertake an investigation in-house, staff will use CMIS to store case notes, logs, actions taken, and details of evidence. It also manages any investigations into organised crime using the same system.

CMIS is also used as an intelligence tool to connect people to properties, weapons, vehicles, images, phone numbers and other individuals. This helps CCC to find relationships and patterns which assist with its investigations. CMIS is also the primary source of information for CCC's reporting, including both internal and public reporting.

Originally developed by the Australian Federal Police, CMIS is now on-sold and supported by a commercial provider.

Audit findings

Poor risk management could compromise the security and reliability of data

We found some gaps in CCC's risk management processes, which could compromise the security and reliability of CMIS data, as well as its availability to those that need it.

Good risk management ensures that CCC can identify, assess and treat risks in a structured fashion. It also ensures decisions around risk are considered and actioned by suitable levels of management.

We noted that:

A risk assessment had not been conducted for CMIS. Without a formal risk assessment, senior management are less likely to understand and plan for risks directly related to CMIS. Given the importance of this system, it is essential that management is aware of the risks to the system, how well it is being protected, and where any vulnerabilities might exist.

CCC had not updated its IT risk register for over 6 years. This means CCC is unlikely to be fully aware of the current risks to its information and the suitability of the controls that are protecting it. Risk registers need to be regularly reviewed and updated to identify new risks and ensure existing risks are properly assessed. CCC's own policies state that risk registers must be updated at least annually.

The 'owner' of the CMIS application is unsuitable, meaning it might not meet the needs of the staff who use it daily. Application owners represent the system's end-users. They should have a good understanding of the business processes supported by the system and be able to make user focused decisions. We found the CMIS owner was part of the information services team. While they will have good technical knowledge of the system, they are not likely to be in a position to advocate for the needs of end users.

Gaps in security controls leave systems and data exposed

We identified out of date, unpatched software vulnerabilities on the server that runs CMIS, as well as other core systems at CCC. An attacker could use these exposed vulnerabilities to gain unauthorised access to CCC's internal network, allowing them to attack internal systems and access highly sensitive data.

We found 218 'critical' and 'highly' rated vulnerabilities that were unpatched for a number of key servers supporting CMIS. These vulnerabilities had more than 100 publicly available exploits.

These patches were missing because of flaws in the process used by CCC to identify vulnerabilities and deploy patches. CCC uses an automated patching system. However it was not set up to patch all the software installed on its computers. An effective patching process that keeps software up-to-date is vital protection against cyber threats and data loss.

We also noted that CCC does not perform vulnerability scans across its IT systems. These scans help agencies find and patch software that is vulnerable or out of date. They are especially useful in finding software vulnerabilities not managed by an automated patching system.

To strengthen security controls, the CCC has implemented ‘application whitelisting’, which the Australian Signals Directorate regards as the number one control to prevent targeted cyber intrusions. This is a list of software applications authorised for use. However, layered security controls, such as patching, restricting administrative privileges and incident and intrusion detection should also be used to make it as difficult as possible for attackers to succeed.

CMIS reporting is limited, requiring manual workarounds

The way the system is designed makes it hard to produce meaningful and dynamic reports for senior management. Staff producing reports use manual workarounds, which put the accuracy of the data at risk and are time consuming.

The reporting features in CMIS are limited, and the system design prevents CCC from directly accessing the CMIS database to query the data.

The system does have a search function that allows data extraction in basic formats. Staff manipulate these CMIS extracts in separate spreadsheets and databases to get the desired output. This takes time and does not provide the flexible or interactive reporting offered by modern data analysis tools.

Lack of disaster preparedness could lead to delays to operations

CCC has identified CMIS as critical for day-to-day operations. An outage of the CMIS application could result in serious delays to operations and CCC would need to go back to a manual, paper-based approach.

We found weaknesses in the following areas that may delay CCC’s ability to recover operations following an incident:

CCC has not yet developed an adequate IT disaster recovery plan for CMIS and other key systems. CCC has recently established a new computer room in a separate location that duplicates data for recovery purposes. However, it does not yet have plans to recover its key systems and it has not done formal testing of the recovery capability.

Backup tapes required to recover CMIS in the event of a disaster have not been tested. This conflicts with CCC’s policy, which requires annual recovery tests. Untested backups may be unreliable or unsuitable.

CCC does not have a continuity agreement in place with its CMIS service provider. If the CMIS service provider is unable to support the system, CCC may not get full access to the system and its data. The CCC should establish continuity agreements to ensure the systems code and other proprietary information is available if the service provider can no longer support the system.

Important processes are not properly supported by policies and procedures

CCC relies on experienced staff members to make sure activities are performed in CMIS correctly and consistently, but lacks sufficient, written procedures to guide their work. Good documented policies and related procedures give clear requirements, roles and responsibilities for the management of IT systems.

We noted gaps in the following areas:

Information security policies were limited. While CCC has implemented many technical controls, it has not properly supported these with policies and procedures. This increases the chance of gaps in its identification and management of security risks.

There is no access control policy and supporting procedures for CMIS. The policies and procedures should guide how new CMIS users are approved and created and how the various user roles are applied in the system. They should also set the requirement for scheduled reviews to confirm that existing CMIS user roles are suitable. Without these, CCC risks providing users with unsuitable access.

There is no formal guidance to ensure data quality. CCC performs some checks to identify data quality issues within CMIS. However, it has not documented responsibilities, frequency of checks, or follow-up activities required. Some issues we noted included misconduct notifications without associated allegations, duplicate entries and assessment decisions incorrectly marked.

Changes to CMIS were not properly managed. We found limited status tracking and reporting of IT changes, change policies that were more than 12 months overdue for review, and CMIS changes that were not logged in the centralised change register. Inadequate change management can lead to unplanned system downtime or misconfiguration resulting in security breaches. However, good 'change management' ensures changes to IT systems are communicated, authorised, tested and implemented in a controlled manner.

Recommendations

1. **By August 2017, CCC should:**

    a. **review and update its information services risk register and conduct an assessment of CMIS to identify risks associated with the information handled and related business processes. This should inform the corporate risk register for senior management to consider**

    b. **review and improve its process to identify and apply software updates to all information systems in a timely manner**

    c. **develop and test disaster recovery plans to ensure the ongoing operations of key applications and IT services. It should also explore continuity agreements with software providers**

    d. **review and update its existing policies and develop new ones to ensure all relevant areas of information security are appropriately addressed**

    e. **review its business needs and assess whether a more suitable application exists for replacing CMIS.**

Response from the Corruption and Crime Commission

The Commission appreciates the importance that adequate controls are in place for corporate applications 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.

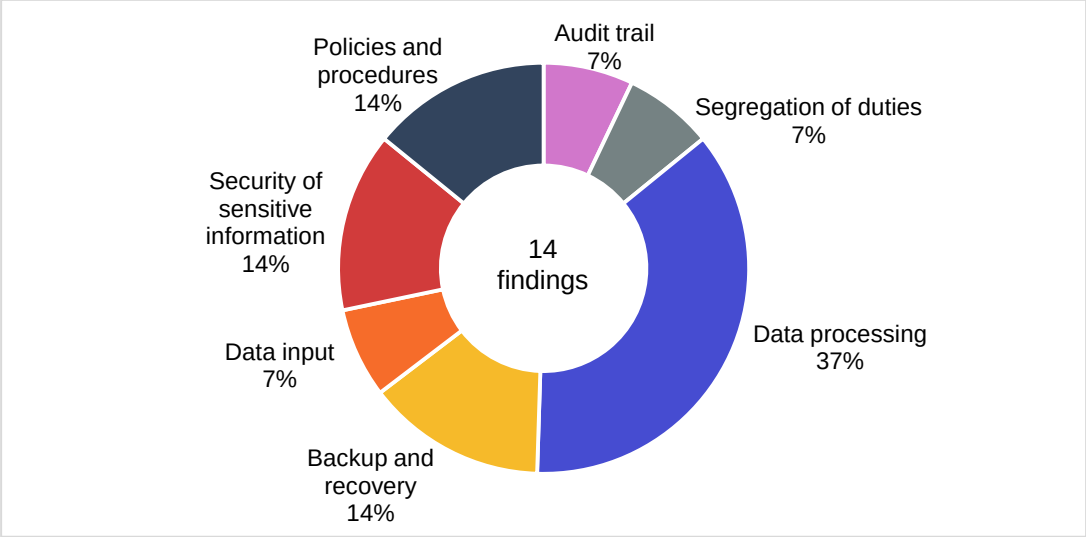
The Commission fully accepts:

- Recommendation (a): By August 2017, the Commission will have completed an IT risk assessment including an updated IT risk register.
- Recommendation (d): The Commission recently completed the review and update of its corporate policy framework. All information security-related policies are anticipated to be endorsed by July 2017.
- Recommendation (e): The Commission's 2016 Information Management strategic plan already outlined the requirement to review and implement a new fully integrated Case Management solution. The CMIS replacement project has progressed well with implementation of a new CMIS system anticipated in 2018.

The Commission accepts in part:

- Recommendation (b): To enhance our existing layered security controls that mitigate risk of cyber-intrusion and unauthorised access, the Commission has recently upgraded its configuration management tool, implemented external vulnerability assessment and a security incident event management tool.
- Recommendation (c): A revised Commission Business Continuity Plan will be completed by August 2017. The Commission has completed a successful IT disaster recovery failover and resolution has been achieved for the continuity agreement with the CMIS provider.

Project and Contract Management (PACMAN) – Department of Finance



Introduction

PACMAN is the system used by the Department of Finance (the Department) to administer projects and associated contracts for the construction of non-residential government buildings. The system contains sensitive data, including banking information of contractors.

Audit conclusion

Overall, PACMAN meets the project and contract management needs of the Department to deliver new non-residential building projects to government agencies.

However, inadequate policies and procedures, and a failure to use some of PACMAN's key functions compromise the accuracy, reliability and transparency of project costs. This increases the risk of under-billed projects and late payments to contractors.

Sensitive data is exposed to unauthorised access or misuse due to inadequate user access management and poor segregation of duties. The Department also risks data loss and downtime in its delivery of key services because it has not properly tested PACMAN's disaster recovery plan to ensure that it is effective.

Background

A key responsibility of the Department is to manage buildings for government agencies and whole-of-government procurement. Building Management and Works (BMW), a strategic business area in the Department, oversees the delivery of new building projects, maintenance of existing facilities, and the provision of office accommodation for government agencies. In 2015-16, BMW was responsible for more than $1 billion of capital works.

BMW has used PACMAN to manage its capital work projects and contracts since 2012. The system supports around 800 active users including BMW staff, external consultants, and contractors providing services.

PACMAN provides automated workflows to guide project managers through the Department's project management lifecycle. This includes a contract register, project activity and timeline management, forecast and cash flow management, payment to providers and billing to clients. PACMAN also integrates with the Department's finance system, which allows payments to be made to contractors and consultants automatically once their work has been completed and approved.

The system was developed by an external IT consultant, who is under contract to provide ongoing support, maintenance and hosting of the system, including data recovery services.

PACMAN's database records for 2015-16 contain:

- 166 projects
- 1,710 contracts (1,193 service contracts and 517 construction contracts)
- 5,488 payment claims for a total of $660,469,451.80 (GST included).

Audit findings

Poor monitoring of project costs has led to distorted budgets and reduced transparency

PACMAN enables project managers to monitor and address any discrepancies between expenditure and income via its budget and cash flow functions. However, managers were not consistently using this functionality.

In our sample of 20 projects, BMW had under-billed 3 projects by a total of $830,127. Another 3 projects still under negotiation, have been under-billed by $857,378. The existing under-billing had already impacted the Department's cash flow. Six projects are 'on hold' because further investigation is required.

Fifteen projects were completed up to 6 years ago, but not finalised in PACMAN nor in the finance system. This delay in finalising project records makes the reconciliation between payments to providers and amounts billed to client agencies more difficult.

In 2016, the Department also identified 2 transactions totalling $855,693 which had become irrecoverable. In both cases, the project management fees had not been billed to the client agency and had to be absorbed by the Department.

BMW needs to ensure that it bills the client agency correctly for their projects. If not, the financial burden will rest with the Department and may result in agencies being unaware of the true cost of their project.

We note that BMW has prioritised the closure of 682 projects and developed new business processes and reporting to monitor and minimise future under-billing of capital works projects.

In 2015-16, contractor payments of over $13 million were paid late

PACMAN has the functionality to generate alerts and reports to prevent payment delays. However, BMW's project managers do not apply these features consistently.

In 2015-16, 45 (4.4%) of the 1,003 payment claims for construction contracts, totalling $13,320,751, were not paid on time. Of these, 98% were paid within 30 days after the due date.

Overdue payments may have a negative impact on the contractor's finances and their ability to provide the engaged services. Late payments may also damage BMW's relationship with contractors, potentially affecting future negotiations.

Australian standard conditions of contract[1] and Treasurers Instructions[2] require agencies to pay contractors no later than 30 days after the invoice is received or goods or services delivered.

[1] AS2124-1992
[2] Treasurer's Instruction 323 Timely Payment of Accounts.

Important transparency and accountability documentation is not properly retained

PACMAN has been designed as a comprehensive project and contract management system that includes a feature to store contract, procurement and other relevant documentation. We found that project managers do not always store key supporting documentation in PACMAN or the Department's electronic document management system. This increases the risk that project requirements are not achieved and also compromises the transparency and accountability for the project, and its procurement decisions.

The Department has also established a checklist of required documentation for each phase of the project lifecycle. This includes standard documents such as a business case and project management plan.

We reviewed 20 projects and noted:

- a project valued over $28 million had no evidence of a business case, project definition plan or project management plan. The business case, in particular, is a critical document and is a prerequisite for budgeting capital expenditure
- another project valued over $43.6 million with no evidence of the procurement options analysis, which is an important transparency tool.

Segregation of duties is not enforced, increasing the chance of errors and mismanagement of projects

There are insufficient controls in PACMAN to enforce segregation of duties, which means that the same user can create and approve a project or a contract.

Adequate segregation of duties decreases the possibility that a single person could be responsible for diverse and critical functions. Without proper segregation, errors or omissions could occur and not be detected in a timely manner and in the normal course of business processes.

During 2015-16:

- 2.4% of the projects had the same person assigned as project manager and project director (4 of the 167 projects)
- 8% of the contracts had the same person assigned as project manager and line manager (43 of the 535 contracts).

The Department's internal auditors also raised this issue in their 2013 and 2016 reports.

Project categories in PACMAN do not align with the Department's policy, allowing inconsistent management practices

Project category, risk levels and other definitions required by BMW do not align with PACMAN. If a project is assigned a lower level category in PACMAN than that determined by policy, it may be under resourced and not given the appropriate level of government oversight.

The 'project category' is an important measure to BMW and the government. It is used to determine the level of governance appropriate to manage the project and the type and degree of detailed documentation required. The BMW project framework designates a project category based on value and risk to government and agencies, which is important for the appropriate management of a project. PACMAN categories are based on billability instead.

The BMW project framework has 5 levels of risk whilst PACMAN only caters for 3. Although BMW has developed extensive user guidelines and training courses for users, PACMAN does not allow users to enter all the project information required by the project framework.

Consequently, PACMAN may provide incomplete information or inconsistent business terminology required for business analysis and decisions. If PACMAN users do not have a full understanding of how the project and contracts are set up, there is an increased risk of inaccurate data input and reporting.

Inadequate access and monitoring controls increase the risk of unauthorised access or misuse

The Department does not have an effective user management process to ensure that only valid users have appropriate level access to PACMAN. This increases the risk of unauthorised access, misuse or inappropriate disclosure of information.

While the Department reviews user accounts on an ad hoc basis and is currently reviewing its project manager accounts, it does not have guidelines on user responsibilities.

The Department only monitors events where a user has been locked out of their account, which is insufficient to provide assurance that events are not due to unauthorised activities. PACMAN has around 350 default audit tables designed by the provider to assist administrators to identify and track unauthorised events. However, the Department was not sufficiently familiar with the audit tables to design a routine logging and monitoring process from the tables and relied on the service provider for ad hoc support.

Without an effective event logging process and proactive monitoring of the logs there is an increased risk that the Department will not be able to detect any unauthorised access or malicious type activity.

PACMAN's disaster recovery plan has not been tested

The Department has not undertaken testing to help verify the effectiveness of PACMAN's disaster recovery plan. Additionally, it is not adequately testing PACMAN's backup media to ensure it can be relied upon in an emergency.

By not testing its disaster recovery plan, the Department has increased the risk that it may not be able to fully restore or recover the system following a major incident or disruption. This may affect business operations and the delivery of key services.

The Department does partially test backup media in response to an application or database change request raised by PACMAN's System Administrator. However, these are not proactively scheduled tests that verify the ability to restore the system from data on backup media.

Recommendations

1. **By August 2017, the Department should:**
    a. **document and communicate business processes to monitor project expenditure/billing and prevent under-billing of capital projects**
    b. **develop a strategic plan, with milestones and responsibilities, to manage 'ready for closure' historic projects**
    c. **periodically monitor payment performance and analyse trends in order to understand the 'root cause' of late payments and reduce incidences**
    d. **fully align PACMAN with the Department's current policies and procedures and record exceptions. Enhance the system's user guidelines in terms of concept description and selection criteria for setting up projects and contracts in PACMAN**
    e. **retain evidence of the review and approval process for the daily reconciliation of expenditure and the monthly billing reconciliation between PACMAN and the financial system.**
2. **By December 2017, the Department should:**
    a. **test PACMAN's disaster recovery plan**
    b. **implement adequate segregation of duties**
    c. **audit the support documentation for its projects to identify gaps.**

Response from the Department of Finance

The Department accepts all the recommendations from the application controls review and provides the following responses:

1(a)	The significant finding (under-billing) has been fully resolved through new reports, processes and additional reviews. The three under-billed projects identified were completed three to five years ago. BMW notes, any under-billing between government agencies does not have an impact on the State's overall financial position.
1(b)	Project closure concerns have been addressed through procedure documents and formal review processes. BMW has fully reviewed and closed all the completed historic projects.
1(c)	BMW notes there are legitimate reasons to hold payments to contractors, which could include legal or contractual disputes. A report has been developed that enables late payments to be investigated. Delays resulting from inefficiencies can then be addressed.
2(a&b)	BMW and the software vendor will update the system in 2017 to address all concerns relating to segregation of duties and disaster recovery.
1(d)&2(c)	Inconsistencies between the Project Management Framework and PACMAN have been resolved. Supporting documentation is also monitored for quality and completeness.
1(e)	Evidence of reviews and approval processes are now retained for all daily and monthly reconciliation processes.

In recent years, BMW has undergone a significant review that has resulted in a more efficient and effective organisation. The audit provided an opportunity to make further improvements.

General computer controls and capability assessments

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 2016 we focused on the following control categories:

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

Conclusion

We reported 441 general computer controls (GCC) issues to the 46 agencies audited in 2016 compared with 454 issues at 45 agencies in 2015.

There was also a decrease in the number of agencies assessed as having mature general computer control environments across all 6 categories of our assessment. Only 7 agencies met our expectations for managing their computer environments effectively, compared with 10 in 2015.

While system change controls and physical security are managed effectively by most agencies, 2 of the categories, information security and business continuity, have shown no improvement in the last 9 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 its 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 and how well developed or capable they should be. 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 46 agencies. This is the ninth year we have assessed agencies against globally recognised good practice.

We provided 41 of the 46 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.

We use a 0-5 scale rating[3] to evaluate each agency's capability and maturity levels in each of the GCC audit focus areas. The models provide a baseline for comparing results for agencies from year to year. This 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 IT operations, IT risks, information security and business continuity. Figure 1 summarises the results of the capability assessments across all categories for the 41 agencies assessed. We expect agencies to rate a level 3 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.

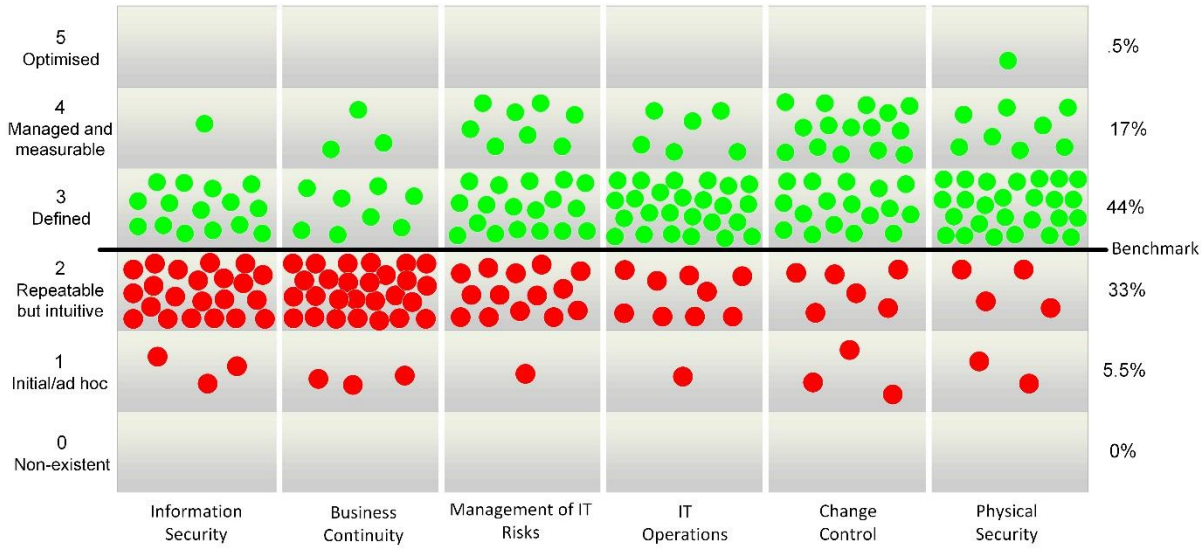


Figure 1: Capability maturity model assessment results

The 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	2015 %		2016 %
Information security	40	↓	39
Business continuity	36	↓	27
Management of IT risks	64	↓	63
IT operations	71	↑	76
Change control	73	↑	78
Physical security	87	↓	85

Table 2: Percentage of agencies at level 3 or above

The results for information security and business continuity were disappointing. They show that 61% of agencies failed to achieve a level 3 or higher in information security and 73% failed to meet level 3 or higher in business continuity.

However, the following agencies have consistently demonstrated good management practices across all areas assessed.

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

Information security

Only 39% of agencies met our benchmark for effectively managing information security, down 1% from the previous year. 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 9 years shows no change to information security controls.

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

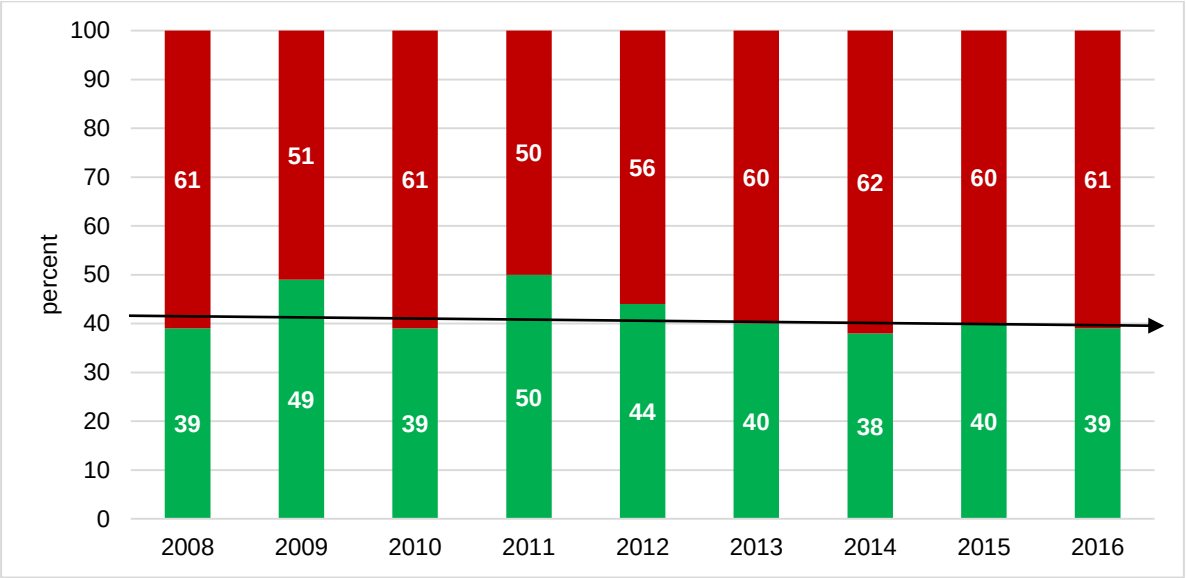


Figure 2: Information security

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
- 100s of sensitive documents shared publicly on the internet due to vulnerabilities
- 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 (more than 11,000 critical and high severity)
- highly privileged generic accounts shared with many staff and contractors, some accounts exist without agency knowledge
- lack of processes and skill to identify security vulnerabilities within IT infrastructure
- no review of highly privileged application, database and network user accounts
- excessive domain administrator accounts – 1 agency had 60 assigned to a contractor
- unauthorised access to systems from the internet by former staff
- not installed or out of date anti-virus software
- default database accounts remain unchanged with credentials widely known and published on the internet.

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. We performed vulnerability assessments and reported over 1,800 critical and 9,200 high severity vulnerabilities on a small sample of key systems to 29 agencies. Security

issues ranged from software updates not being applied to weak passwords, malware infections, unauthorised access and disclosure of sensitive and confidential information.

We also performed tests that demonstrated that agencies failed to detect the loss of information from 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 found security weaknesses in an agency's website that contains sensitive information on children. These weaknesses allowed us to access information including children's names, birth dates and suburbs they reside in. With this access we were also able to generate invoices and adjust the status of external business submissions for funding. In addition, the website login credentials were displayed in plain text over the internet. The agency locked down the website after we notified them of the issue.

Figure 3: Website vulnerabilities provide access to agency systems

Unsupported operating systems

One agency uses an in-house developed tool to share documents. A vulnerability in this tool allows anyone to view documents via the internet. We viewed 200 documents and discovered information such as internal investigation reports and employee job application outcomes without requiring any authentication. These documents also contained sensitive information such as names, addresses, network account names and system information. This tool was hosted on an unsupported version of operating system which would also be susceptible to other exploits.

Figure 4: Unsupported operating systems allow unauthorised access to sensitive information

Inadequate termination controls

At one agency we found an instance where a former staff member was logging on to IT systems months after their termination. We notified the agency of this issue and they could not establish what actions the former employee performed or why. Without appropriate user access management controls there is an increased risk of inappropriate or unauthorised access.

Figure 5: Terminated staff still have access to systems

Default credentials were not changed

We found a number of devices on the network with default usernames and passwords at an agency that collects and manages a significant amount of critical information for government and the public. These initial login credentials are setup by the manufacturers and as good practice should be changed during the configuration processes. We saw network switches, routers and remote management systems with default credentials. Using default credentials, we were able to logon to a remote system with full administrative privileges. This system is used for server hardware maintenance.

Figure 6: Default credentials could enable administrator level access

Passwords were stored in plain text

During our audits we view documented IT policies and procedures. In one instance, we found sensitive passwords stored in plain text in one of the IT procedures. These included high privileged domain administrator account credentials, remote access (VPN) service logon credentials and access to the messaging system. We tested the credentials and these allowed us to access the Department's messaging system from the internet. A malicious user can intercept or read any communication with departmental staff. As a good practice passwords should not be stored in plain text documents.

Figure 7: Storing passwords in plain text allows unauthorised access to systems

Easy to guess passwords

In 2015 we reported being able to log into a department's network by guessing the password, which was 'password'. This account could access thousands of sensitive documents. One year later, when auditing the agency again, we attempted to login to this same account with the same password ('password'). We were again successful, however we did note the network was more secure and the sensitive documents were no longer accessible.

Figure 8: Sensitive information is at risk when passwords are easy to guess

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.

We examined whether plans have been developed and tested. We found a 9% reduction from last year with 73% of the agencies still not having adequate business continuity and disaster recovery arrangements in place. The trend over the last 9 years has shown agencies are not affording sufficient priority to disaster recovery and continuity.

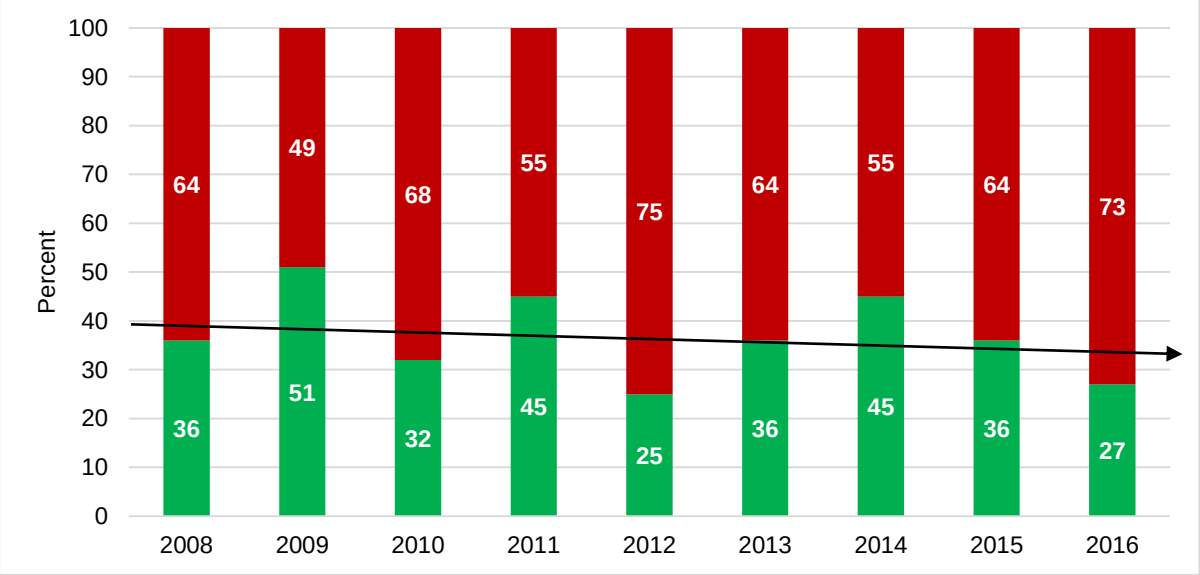


Figure 9: Business continuity

Weaknesses we found included:

- no BCPs
- BCPs in draft or not reviewed for many years
- tolerable outages for critical systems not defined
- no DRPs
- old and redundant DRPs with some not reflecting current ICT infrastructure
- DRPs never tested
- 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

Sixty-three percent of agencies met our expectations for managing IT risks, a 27% improvement since the first assessment in 2008, with agencies showing improved management controls over risks.

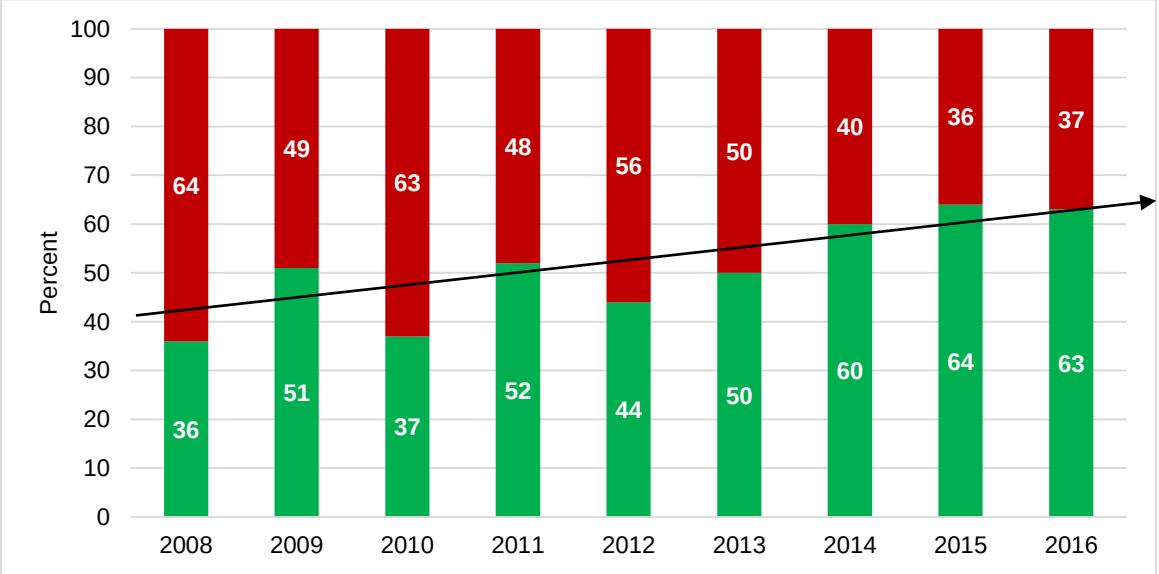


Figure 10: Management of IT risks

Weaknesses we found included:

- risk management policies in draft or not developed
- inadequate processes for identifying, assessing and treating IT and related risks
- no risk registers
- 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' increased 5% in 2016 compared to the previous year. However, there has been overall improvement of 28% since 2011.

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 effectively working
- 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.

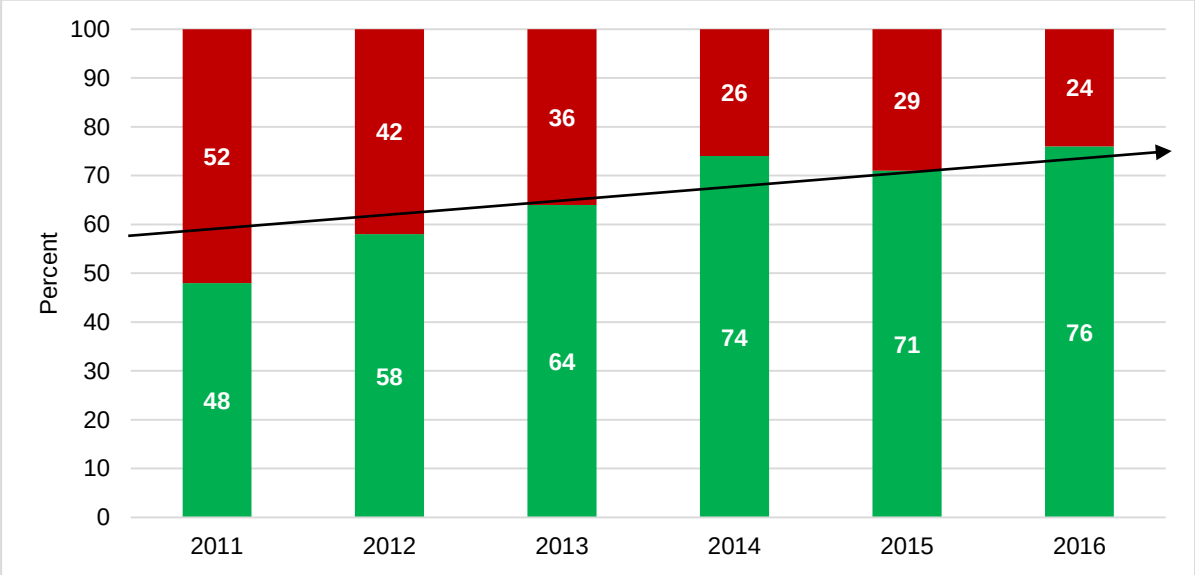


Figure 11: IT operations

Weaknesses we found included:

- information and communication technology strategies not in place
- no logging of user access and activity on critical systems or sensitive data
- network logs only kept for short periods, e.g. 1hr to 4 days
- former staff with access to agency networks and applications years after termination
- unauthorised devices can connect to networks, such as USBs and portable hard drives

- no reviews of security logs for critical systems including remote access and changes to databases with confidential information
- lack of policies and procedures
- cloud solutions adopted by staff without approval
- several agencies are running unsupported operating systems
- no user education of security policy and security related responsibilities and induction processes not implemented or followed
- no incident management procedure
- asset registers not maintained and ICT equipment unable to be located.

The above 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 32 out of the 41 agencies achieving a level 3 or higher rating.

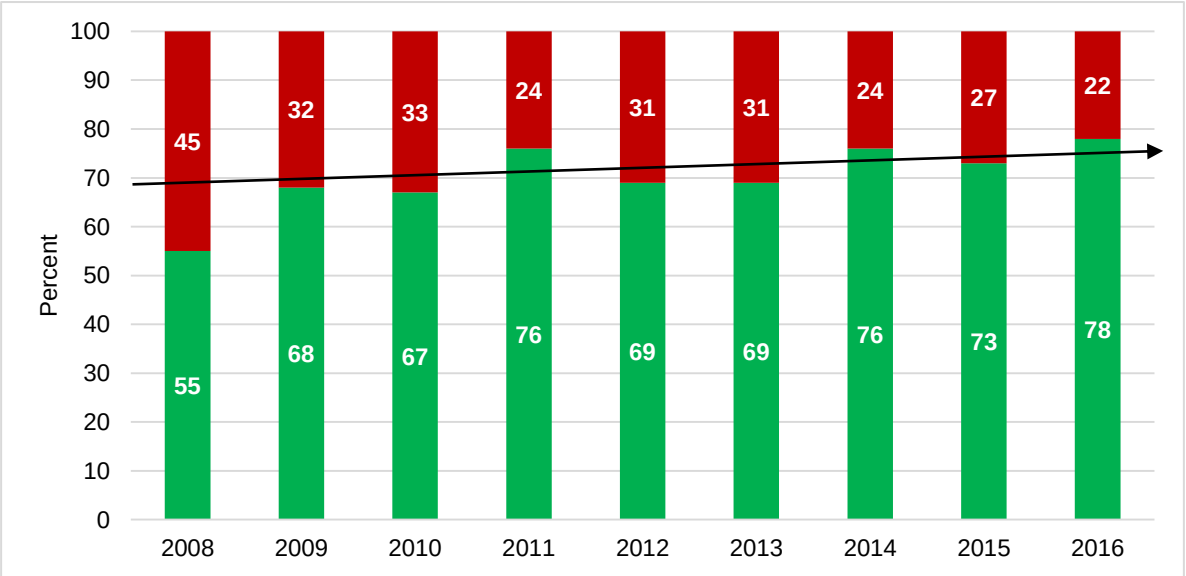


Figure 12: Change control

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

- individuals are able to request and approve their own changes
- change control groups exist but have never met to manage or consider changes
- changes affecting staff are not communicated.

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.

Six of the 41 agencies fell below our expectations for the management of physical security.

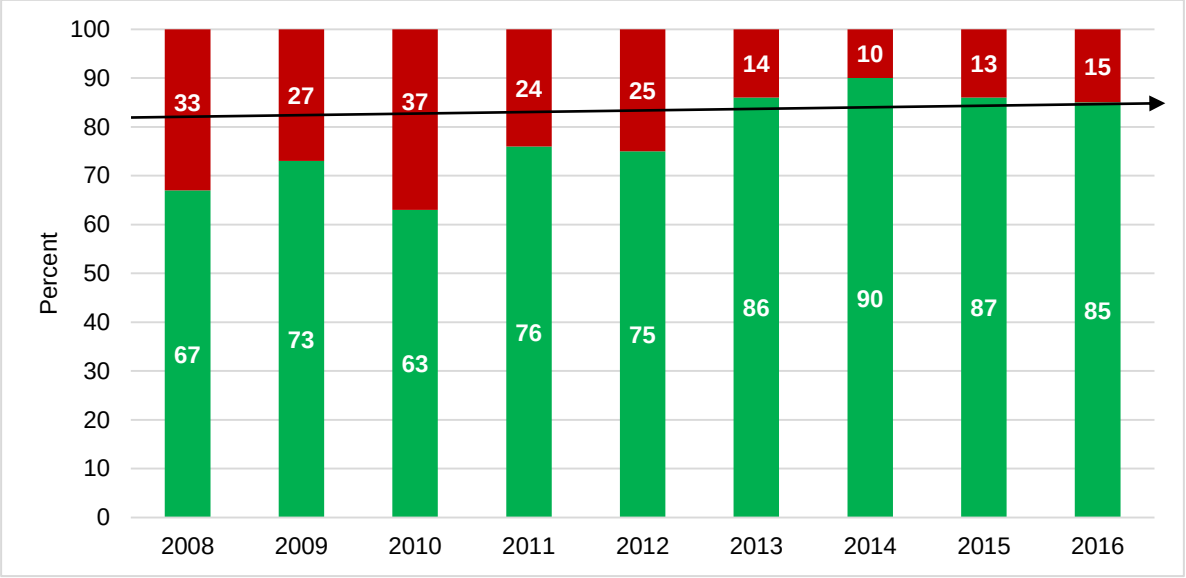


Figure 13: Physical security

Weaknesses we observed included:

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

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 14 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.

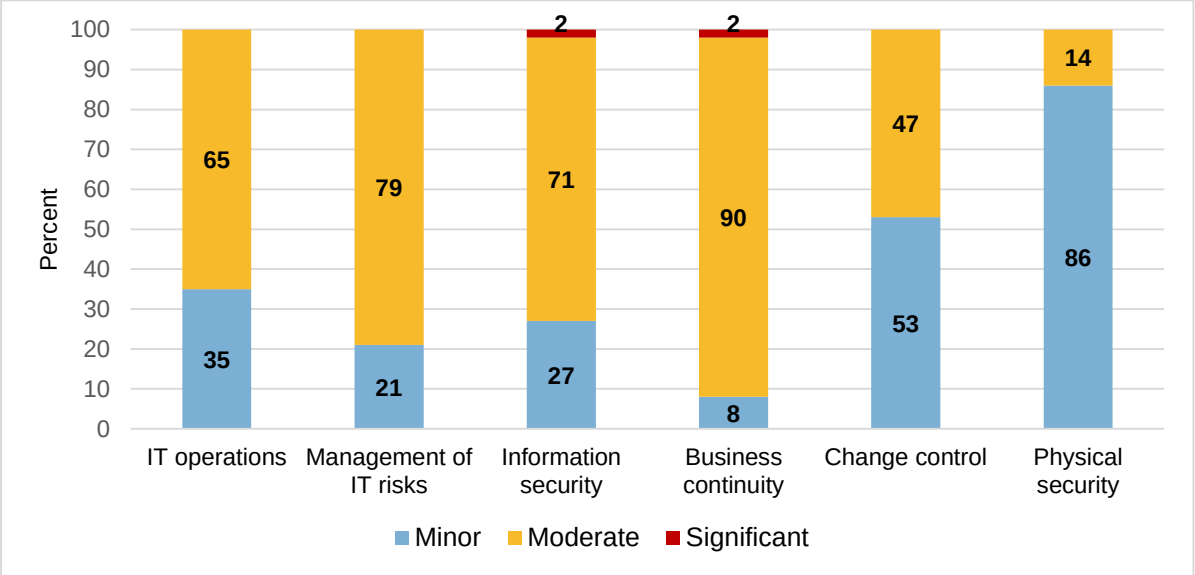


Figure 14: Distribution of ratings for the findings in each area we reviewed

Recommendations

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 must conduct ongoing reviews of user access to systems to ensure they are appropriate at all times.

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.

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.

Management of 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. We recommend the use of standards and frameworks as references to assist agencies with implementing good practices.

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.

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	2017 reports	Date tabled
11	Opinion on Ministerial Notification	29 June 2017
10	Timely Payment of Suppliers	21 June 2017
9	Opinion on Ministerial Notification	8 June 2017
8	Management of Medical Equipment	25 May 2017
7	Audit Results Report – Annual 2016 Financial Audits – Universities and TAFEs – Other audits completed since 1 November 2016	11 May 2017
6	Opinions on Ministerial Notifications	13 April 2017
5	Accuracy of WA Health's Activity Based Funding Data	11 April 2017
4	Controls Over Purchasing Cards	11 April 2017
3	Tender Processes and Contract Extensions	11 April 2017
2	Opinion on Ministerial Notification	6 April 2017
1	Opinion on Ministerial Notification	30 March 2017

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