Western Australian
Auditor General's Report

Information Systems Audit Report

Report 11: June 2016

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.

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

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Information Systems Audit Report

Report 11
June 2016

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
22 June 2016

Contents

Auditor General's overview

This is my eighth annual *Information Systems Audit Report.* The report summarises the results of the 2015 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. It also contains recommendations that address these common weaknesses and as such, has a use broader than just the agencies we audited.

The first item of the report contains the results of our audit of key business applications at 5 agencies. Most of the applications we reviewed were working effectively. However, all 5 had weaknesses, the most common of which related to poor policies, procedures and security. The potential effect of these weakness is the compromising of sensitive information. We also found weaknesses in operational, procedural and process controls that could potentially impact delivery of key services to the public.

The second item presents the results of our general computer controls and capability assessments of agencies. There was a slight decrease in the number of agencies assessed as having mature general computer control environments across all 6 categories of our assessment. The number of agencies that failed to meet our expectations for 3 or more of these categories increased. Overall, the result was a slight decline from the previous year.

We have been reporting the capability assessments for a number of years and for the first time have included a trend line for each of the categories. Disappointingly, 2 of the categories have shown no improvement in the last 8 years. These continue to be affected by easy to address issues such as poor password management and ensuring processes to recover data and operations in the event of an incident are kept updated.

My practice is not to name agencies that have information system weakness for fear that this could encourage attempts to exploit the weaknesses. However, I am now reviewing that position and seeking advice as to whether the naming of high-risk agencies is necessary in order to achieve essential change.

Application Controls Audits

Introduction

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

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

What did we do?

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 is not managed appropriately.

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

- Appropriate **policies and procedures** are in place to support reliable processing of information
- Controls over **data preparation, collection and processing of source documents** are accurate, complete and timely before the data reaches the application
- **Data entered** into the application is accurate, complete and authorised
- **Data processed** as intended in an acceptable time
- **Data output** including online or hardcopy reports are accurate and complete
- **Interface controls** are suitable to enforce completeness, accuracy, validity and timeliness of data transferred
- Controls over **master file integrity** are effective which ensure changes are approved, accurate and complete
- Controls over **transaction logs** ensure transaction history is accurate and complete
- **Duties are segregated** and no staff perform or are capable of performing incompatible duties
- The system/application is **backed-up** and can be **recovered** in the event of a disaster

The 5 agency applications we reviewed were:

1. **Complaints and Licensing System (CALS)** – Department of Commerce
2. **Total Offender Management System (TOMS)** – Department of Corrective Services
3. **Controlled Waste Tracking System (CWTS)** – Department of Environment Regulation
4. **Smart Parker** – Public Transport Authority
5. **Treasury System** – Gold Corporation

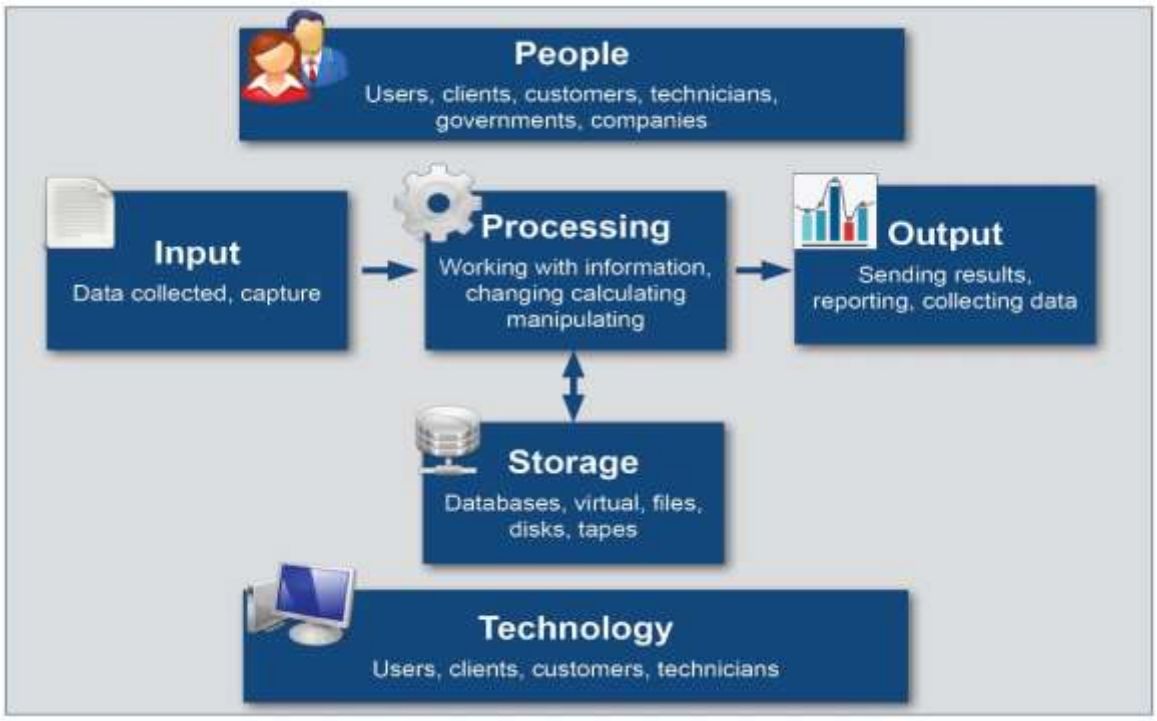


Figure 1: Key elements of focus for our application reviews

Figure 1 represents the focus of our application reviews – people, process, technology and data. In considering these elements, we follow the data from input, processing and storage, to outputs.

Overall assessment

All 5 applications had some control weaknesses with most related to poor policies, procedures and the security of sensitive information. We also found issues with operational, procedural and process controls that aim to ensure the applications function efficiently, effectively and remain available. We found 56 findings across the 5 applications with 6 rated as significant, 39 moderate and 11 being minor. Correcting most of the issues we raised is relatively simple and inexpensive. Figure 2 shows the findings for the 5 applications reviewed.

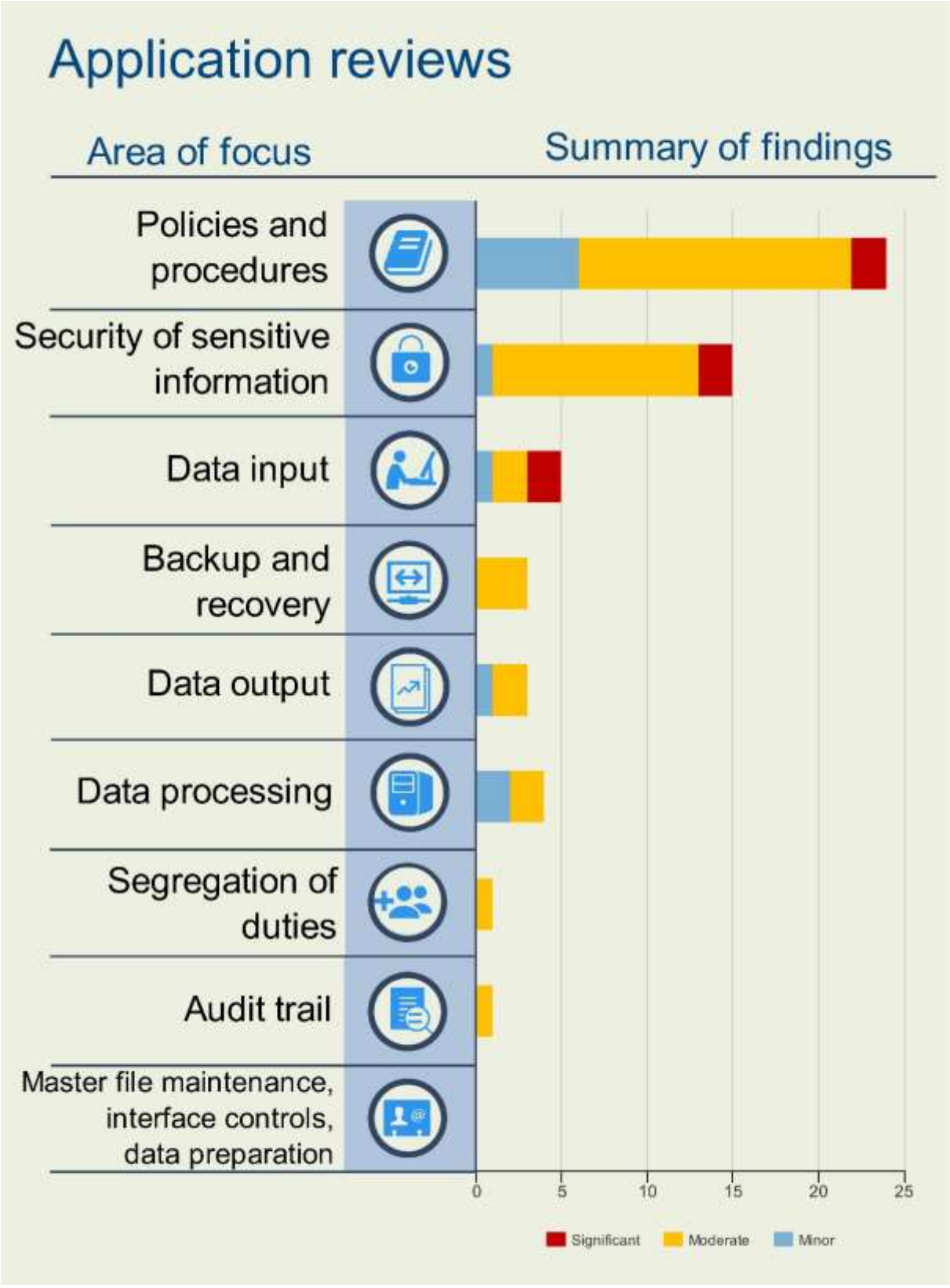


Figure 2: Application reviews

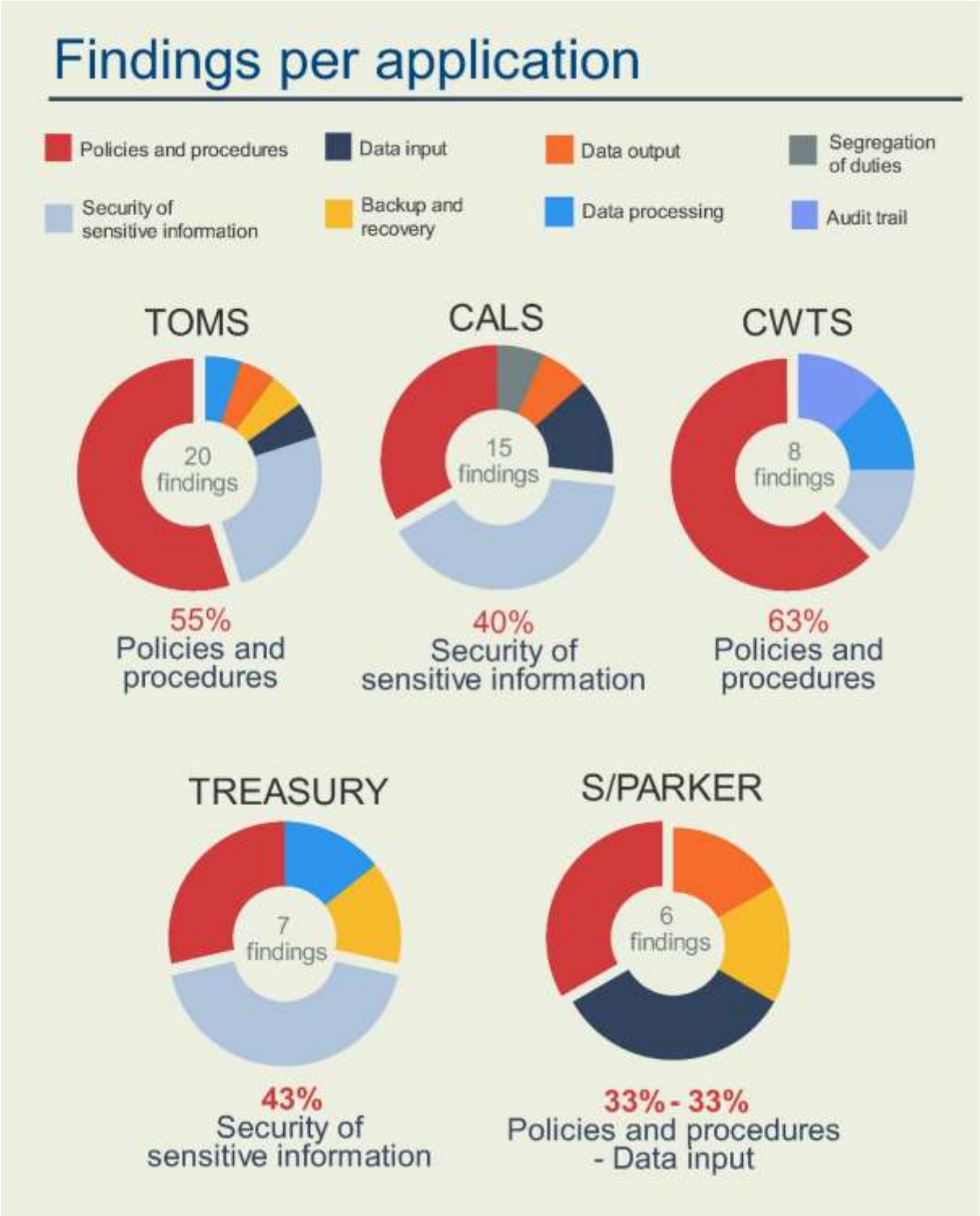
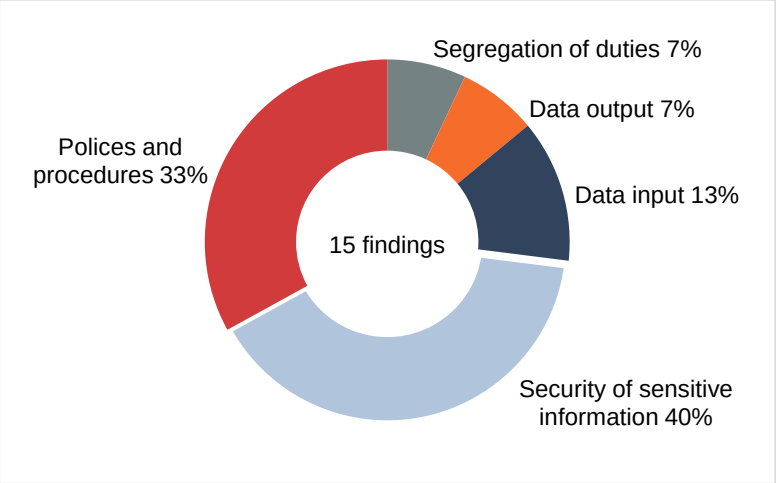


Figure 3: The areas of findings per application

Complaints and Licensing System – Department of Commerce



Background

The focus of our audit was the Department of Commerce's (Commerce) Complaints and Licensing System (CALS) which holds information on approximately 760,000 clients and processes over 10,000 licences and 1,000 complaints every month. It also generates key performance indicator (KPI) information for annual reports.

Commerce has a critical role in safeguarding the interests of consumers and in regulating various professions. The 4 divisions at Commerce that provide licensing services (EnergySafety, Consumer Protection, Work Safe and the Building Commission) issue 47 different types of licences covering a range of professions such as builders, electricians, motor vehicle repairers, real estate agents and employment agents.

Commerce developed CALS in-house to process licences. Consumer Protection and the Building Commission also use CALS to record and investigate complaints made against licence holders and others.

To process licence applications, Commerce collects information from applicants using paper-based forms. The forms are checked for completeness then entered into CALS. Applicants for some types of licence may also need to submit supporting documentation such as proof of identity, qualifications, certifications, and criminal history checks. Building Commission scan these documents into CALS.

Once all the required information is in the system, workflows guide staff through the process of reviewing the eligibility of applications and issuing licences. Commerce uses a third party to print some licences, though this requires the sharing of some applicant information.

Conclusion

The CALS application is largely effective at enabling Commerce to manage licences and complaints.

However, a weakness in functionality has seen licences issued for a length of time that exceeds the regulatory period of licence. As well, sensitive personal information collected in CALS is at some risk due to the use of insecure transfers of information over the internet to a third party and database vulnerabilities that increase the risk of unauthorised access.

Audit findings

Licences are issued for longer than the correct periods

A fundamental purpose of CALS is to issue licences to eligible persons for periods stipulated by regulations. However, we identified a functionality weakness with CALS that can result in the issuing of licences for incorrect periods.

While our sample identified only a small number of these errors, it is sufficient to raise concerns. Our analytics-based review of about 8,000 licences identified 22 errors including:

- licences issued with the start date set well in the future, in one instance up to 5 years in the future
- a high risk (forklift, scaffolding, cranes and hoists) licence issued in August 2015 with an expiry date of 2025. Regulations limit this type of licence to 5 years
- a plumber's licence issued in June 2015 with an expiry date of 2021. Regulations limit this type of licence to 3 years.

We also identified 74 licences created for testing purposes. These appeared as valid licences on Commerce's website and are present in published licence registers.

Data integrity is a fundamental requirement of a licensing system with potential ramifications for business operations and staff efficiency. One potential consequence of incorrect licence periods is that Commerce will not conduct the required regular checks on licence holders to verify that they continue to comply with licence conditions.

Security of electronic records

Protection of sensitive personal information is an important requirement of a licensing system. In our view, there is inadequate protection in CALS of sensitive information such as full name, address, date of birth, applicant photo, licences, investigation papers and decisions, credit reports and complaint details of individuals and organisations.

Some of the weaknesses we noted were:

- **Sensitive information is insecure** – there are inadequate security controls for the CALS working data files. These files are stored on open network files, outside of CALS. The security restrictions in CALS do not apply to these network files, and no other controls restrict access. All staff connected to the network have full access to view, modify and delete these files. This may result in data being accidentally or deliberately modified, copied or deleted.
- **Sharing data with third parties** – WorkSafe shares sensitive information with a third party using an insecure file sharing portal. The portal does not require a username or password to download files and sent data is not secured through encryption. We also found that the Building Commission emails renewal notices to a third party for printing and dissemination. This information includes names, date of birth, email addresses, contact numbers, addresses and/or applicant pictures. Email is not encrypted or secured and is vulnerable to interception. Although Commerce has access to a secure data sharing system, not all staff and divisions are aware of this facility. Sharing sensitive information with third parties without adequate security controls increases the risk of data theft.
- **Credit card information may be at risk** – Commerce's branch offices scan and email hard copy licence applications to Head Office for processing. These email messages often include the full credit card number and payment details of the applicant. We found

many of these email messages archived into Commerce's recordkeeping system without the credit card details removed or redacted.

Processing and storing credit card information without appropriate levels of protection significantly increases the risk to Commerce and the individuals concerned and is in breach of Payment Card Industry Data Storage Standards (PCI-DSS). Unprotected credit card information may be misused or compromised.

- **Passwords were easily guessed** – we identified multiple database accounts with very easy to guess passwords. Examples include passwords that were same as the username and passwords such as 'welcome1' and 'password1'. We also found that password aging was not enforced, the password of an unrestricted administrator account was unchanged for over a year and a large number of inactive system accounts have not had their default passwords changed. Easy to guess passwords are inconsistent with good practices and lead to unauthorised access.
- **Software updates not applied** – the CALS database was not 'patched' with critical software updates released by the vendor to fix known security vulnerabilities. Attackers can exploit known vulnerabilities and potentially gain access to the system and to sensitive information.
- **Database activities not logged** – Commerce has not established database logging and auditing to monitor and record system changes made at the database level. As a result, changes to the database cannot be traced back to individuals and any suspicious modification or access to data will go unnoticed.

Segregation of duties

We found inadequate controls around the processing of licences within the EnergySafety division. A licensing officer performs the complete licensing process. This involves entering the licence application, approving the licence and printing out the licence card. Standard control procedures usually involve a segregation of duties to prevent or detect any inappropriate issuing of licences.

Manual data entry and processing

On average Commerce will process over 10,000 licence applications and renewals, and 1,000 complaints every month. All new licence applications, and the majority of renewals, are manually entered into CALS. Manual data entry compared to automated entry is inefficient and the completed data set is more likely to be inaccurate and/or incomplete.

Commerce currently has an online facility for lodging some renewal applications, but there is no facility to lodge new applications electronically or online. However, Commerce has a project to move all licence applications online by 2018.

Other findings

Commerce does not have a formal policy to govern software development standards and processes. A comprehensive policy better enables entities to control the risks that affect the costs, timescales and quality of projects. The need for a policy is raised given that CALS is an in-house developed system and Commerce does not have an enterprise level diagram to show business processes supported by the CALS application. Detailing key business processes identifies opportunities and efficiencies which is particularly important given the size and complexity of CALS.

The CALS application and associated processes has not undergone a risk assessment. Without an adequate risk assessment, senior management are less likely to understand and plan for risks related to the information they are responsible for managing.

Commerce does not have an access control policy and supporting procedures for CALS. In the absence of this, we found:

- A number of staff using one administrator account, decreasing the capacity to identify individuals (if necessary) that modified data either deliberately or unintentionally. Accepted good practice is for administrators to have their own accounts rather than a shared account.
- An account with administrator access without any formal approval. Administrators can change security settings, install software and hardware, and access all files. For this reason, administrator access should be authorised.
- Testing of a sample of 18 CALS users showed that the accounts of 3 former employees were still open. The failure to terminate access of former employees represents a fundamental breakdown in control.

Recommendations

By December 2016 Commerce should:

1. **review the information security policy to ensure**
    a. **access management for systems is defined**
    b. **appropriate controls are in place to protect sensitive information**
2. **establish appropriate controls to ensure accurate data entry of licence expiry and renewal dates**
3. **undertake a risk assessment of CALS**
4. **review the licensing process within the EnergySafety division**
5. **develop and implement an IT software development policy**
6. **consider automated processes for capturing and managing licence data.**

Response from the Department of Commerce

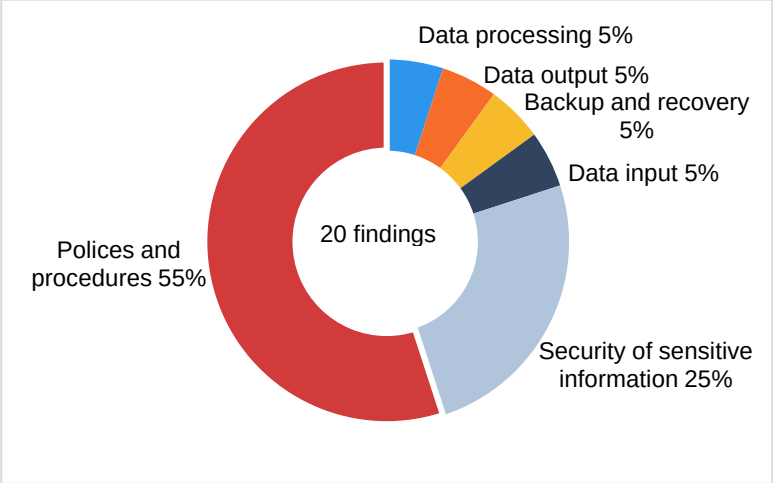
The Department of Commerce (Commerce) welcomed the performance review of application controls for the Complaints and Licensing System (CALS). CALS was originally developed as an information system to underpin regulation of the real estate industry and over time has been applied as the default licensing tool across four divisions of Commerce.

The audit analytic tool was especially useful in identifying two data integrity issues that had not previously been detected. These were immediately rectified and no known detriment or misuse is believed to have occurred.

Commerce accepts recommendations (2) and (5) regarding accurate data entry and IT development policy, and has taken steps to implement both. Recommendations (1) and (6) regarding information security and automation of processes are accepted and will be implemented in the move to an online licensing environment by 30 December 2017. Recommendations (3) and (4) regarding a risk assessment of CALS and review of EnergySafety licensing processes are accepted and will be implemented by 30 September and 30 December 2016 respectively.

Commerce has commenced a significant initiative to move all of its major licensing activities to a new Commerce Online Occupational Licensing system to be rolled out during the period 1 July 2016 to 30 December 2017. With this impending change, the opportunity to address any underlying issues is appreciated.

Total Offender Management System – Department of Corrective Services



Background

The Department of Corrective Services (DCS) aims to provide safe, secure and meaningful corrective services that contribute to community safety and reduced offender involvement in the justice system. Over 4,000 staff work across the state at approximately 50 locations in Western Australia, managing adults and young people in prisons, detention centres and in the community.

DCS heavily relies on a custodial information application – Total Offender Management System (TOMS), to meet its responsibilities.

TOMS is the main information source for management of adult prisoners and young people in the community. If TOMS data is unavailable or incorrect, there is an increased risk to the safety of offenders, DCS staff and the community.

A number of other agencies, including the Prisioners Review Board, Department of the Attorney General and WA Police also rely on specific data from TOMS, such as location of prisoners, demographic details, discharge information and assessment reports. Oversight bodies such as the Corruption and Crime Commission and the Office of the Inspector of Custodial Services also rely on data from TOMS as evidence of activies.

On a typical working day, around 1,400 users access TOMS. The total number of users, located throughout Western Australia, is in excess of 4,600. Implemented in 2001, the TOMS database contains records generated since 1954 including:

- 78,000 prisoners (6,000 active)
- 10,000 young people in detention (150 active)
- 77,000 young people in the community (1,700 active)
- 500,000 persons who visited offenders in prison.

These records contain large amounts of sensitive information including personal identification, sentence details, health, counselling and incidents (including serious assaults), for adult and young offenders. TOMS is the primary source of information for DCS reporting. This includes key performance indicator data, operational reports and information for third parties including Parliament, the Ombudsman and the Australian Bureau of Statistics.

Conclusion

Overall, TOMS meets the needs of DCS staff to manage offenders in correctional facilities and the community.

However, several manual processes cause data integrity issues that require continuous correction by DCS. One of the causes of the data integrity problems has been addressed, which should ensure greater accuracy of data, but historical inaccuracies remain and will only be resolved with time. In addition, we identified a number of system and database vulnerabilities that increase the risk of unauthorised access to electronic information relating to prisoners and young offenders.

Audit findings

The integrity of the system is at risk from inaccurate information

Users of the TOMS application identify large numbers of data integrity issues on a daily basis. For instance, between 9 November 2014 and 8 November 2015, more than 2,350 data integrity issues were recorded. These issues are primarily caused by manually entered data. Given the large volume of data manually entered it is likely that many errors remain unidentified.

Examples of integrity issues, many of which occur when prisons first receive offenders, include:

- offenders entered multiple times
- incorrect offender details such as name or date of birth
- incorrect recording of incidents involving offenders
- missing photos or the photo of a different person is recorded

In some cases these errors occur because the documentation the Department relies on when it receives offenders contains incorrect information.

DCS staff advised that some types of error such as medical, behavioural and mental health information, including self-harm potential can increase the risk to DCS staff and offenders. Incorrect information can also have a negative impact on staff efficiency and DCS operations. However, there are compensating controls outside of TOMS that mitigate this risk.

Some recent automation will help improve accuracy

Various manual processes for data entry, data manipulation and reporting have adversely affected the accuracy and reliability of TOMS information and reports. Some automation has occurred but problems remain.

Figure 4 is an example of manual processes that contribute to data errors.

DCS staff are required to report incidents which may jeopardise the security of the prison or the welfare or safe custody of prisoners. Following an incident, DCS staff manually enter into TOMS the incident details that should include the type of incident, category, location, time, description and persons involved. Although there are checks of the data input, it is not always possible to determine if an input error had been made. DCS advised that approvals through the chain of command mitigate this risk.

Errors in the recording of incidents is a main cause of corrections to TOMS. Between 9 November 2014 and 8 November 2015, 422 corrections were made in this area.

Errors can have serious consequences. For instance, decisions based on incorrect incident information may result in necessary follow-up activities not occurring. These activities include changes to prisoner risk assessments and charges or penalties for prisoners involved. However there are compensating controls outside TOMS that mitigate this risk.

Incorrect incident information will also increase errors in the DCS reporting processes, including that of a key performance indicator – the rate of serious assault. DCS advised that quality assurance processes are in place for all key performance indicators to support the accuracy of reporting.

Figure 4: Manual entry of incident information

DCS is working to improve the data integrity issues. For example, a main cause of inaccurate information was the manual input of warrant information. Warrants detail the identity of the offender, charges and the sentences imposed. Until October 2015, this information was manually entered into TOMS. DCS automated the process and introduced a manual check back to the hard copy warrant form. These controls are expected to increase the accuracy of warrant information in TOMS, although it will take time for historical errors to be identified and corrected.

DCS also manually extracts TOMS records and manipulates the data to provide information and reports that TOMS has not been designed to produce.

Sentence details are extracted from TOMS and manually entered into a spreadsheet. The spreadsheet uses the sentence information to calculate dates for various reviews and release of prisoners. These dates are then manually entered back into TOMS. Incorrect dates mean that DCS relies on other manual processes to ensure prisoners are released on time. The initial sentence calculation is audited by a second person who checks all of the calculations involved in a prisoner's current term from start to finish before it is entered into TOMS.

DCS reports its key performance indicator and operational statistics using a largely manual process:

- to ensure all reports use the same point in time information, data in TOMS is automatically transferred to a data warehouse
- accurate delivery of overnight data is validated by cross referencing with source systems when producing reports
- the statistical analyst runs queries that generate reports and information on the warehoused data
- the numbers generated by these queries are manually entered into a spreadsheet, for example, daily prison population at midnight
- the spreadsheet is used to collate and calculate various daily statistics

- DCS uses the data in the spreadsheet as the source of official KPI and operational statistics
- DCS advised that the data is compared for consistency against previous quarterly and annual statistics.

Manual processes are inefficient and increase the risk of inaccurate and/or incomplete information and reports. DCS may also report inaccurate KPI information and operational statistics.

Security of sensitive information

We performed a vulnerability assessment and database security check on the TOMS application and the supporting IT environment. These tests identified a range of weaknesses which increase the risk to the confidentiality, integrity and availability of sensitive DCS information.

Some of the weaknesses we noted were:

- **Software updates not applied** – we found that software updates released by the software vendors to fix known security issues and weaknesses were not applied to the TOMS database, application and other critical servers. Without these updates, attackers could exploit known vulnerabilities and may gain access to systems and information. An effective patching process that keeps software up-to-date is vital protection against cyber threats and data loss.
- **Unsupported operating systems** – servers run operating systems that the vendor no longer provides security updates for or supports. This increases the risk of DCS's IT systems and information being compromised.
- **Vulnerability assessments are not conducted** – DCS does not perform vulnerability assessments across their IT systems and therefore cannot give assurance that its software updates are applied correctly and are not vulnerable to threats.
- **Account sharing** – the highly privileged database administrator account is shared by 15 different people including 12 contactors that support the TOMS application. This sort of arrangement is inconsistent with accepted good practice as the use and activities of this account cannot be traced back to specific individuals.
- **Database passwords do not expire** – database user account passwords are not set to expire. We found a number of users had not changed their passwords in over 5 years, including the password for the database administrator account. DCS runs a significant risk that individuals who are no longer authorised to access TOMS information may do so through the shared administrator account. Configuring passwords to expire periodically reduces this risk.
- **Database activities not logged** – DCS has not established database logging and auditing to monitor and record system changes made at the database level. As a result, changes to the database cannot be traced back to individuals and any suspicious modification or access to data will go unnoticed.
- **Backups not encrypted** – TOMS backups are not encrypted. Backups are stored on tapes that are collected and managed by a third party contractor. This creates a risk of unauthorised access and inappropriate disclosure of DCS information if tapes stored offsite are misplaced or stolen. Encryption of backup media, where confidentiality is of importance, is also in line with the international standard for information security (ISO27002/2013).

Sensitive information is stored in insecure locations

DCS has inadequate security over both the hard copy and electronic copy of confidential Court warrants.

DCS stores the hard copy warrants in unlocked cabinets in an open plan office. The electronic copies are stored in a shared email system that lacks proper document management. These records contain the identity of the offender (including that of young offenders) the criminal charges and the sentences imposed.

Inadequate security creates the risk of unauthorised access and distribution.

Controls to ensure ongoing operations

TOMS is crucial to DCS day-to-day operations. If TOMS was unavailable, DCS would be forced to use paper-based records to manage critical functions including prisoner counts and movements such as between prisons and courts, visitor information and prisoner risk/threat assessments. The unavailability of TOMS would increase the safety risk to DCS staff, visitors and offenders.

We identified a number of issues that may impact the availability of TOMS:

- DCS has not performed a risk assessment of TOMS and its supporting business processes. Without an adequate risk assessment, DCS will not be able to identify, assess and treat risks that affect the successful operations of TOMS.
- DCS has not yet developed an IT disaster recovery plan for TOMS and other key systems. This means that DCS may be unable to recover the TOMS application in a timely manner to ensure minimal disruption to operations.
- DCS has not tested the backup tapes it plans to use to recover TOMS in the event of an incident. It is therefore uncertain that TOMS can be recovered if required.
- Although each DCS facility has its own business continuity plan, it does not have a BCP for DCS head office. The majority of TOMS support and administration staff are based at this office. In the event that systems become unavailable, there is no documented plan on how the department will operate.
- The DCS change management process does not adequately capture and assess the impact of changes to TOMS. Changes can be made at the request of an end user without appropriate stakeholder oversight and approval, thereby creating a risk to the availability and security of TOMS.

Recommendations

1. **By August 2016 the Department of Corrective Services should:**

    a. **Undertake a risk assessment of TOMS to identify risks associated with information handled within TOMS and related business processes. This should inform the corporate risk register for senior management to consider.**

    b. **Ensure that appropriate controls are in place to protect the information stored in databases and systems to prevent exposures that could lead to the compromise of information. This should include a process to identify and apply software updates to all information systems in a timely manner. Consideration should be given to risks with outdated and unsupported operating environments.**

    c. **Ensure sensitive hard copy information is adequately secured.**

2. **By December 2016 the Department of Corrective Services should:**

    a. **Ensure all data entry processes have appropriate controls to ensure the accuracy and integrity of information.**

    b. **Review the existing data integrity issues within TOMS to ensure accuracy and completeness. This can also be used to identify the source of errors.**

    c. **Produce a business continuity plan for head office and a disaster recovery plan to ensure the ongoing operations of key applications and IT services. These plans should be tested to ensure they will operate effectively.**

3. **By June 2017 the Department of Corrective Services should:**

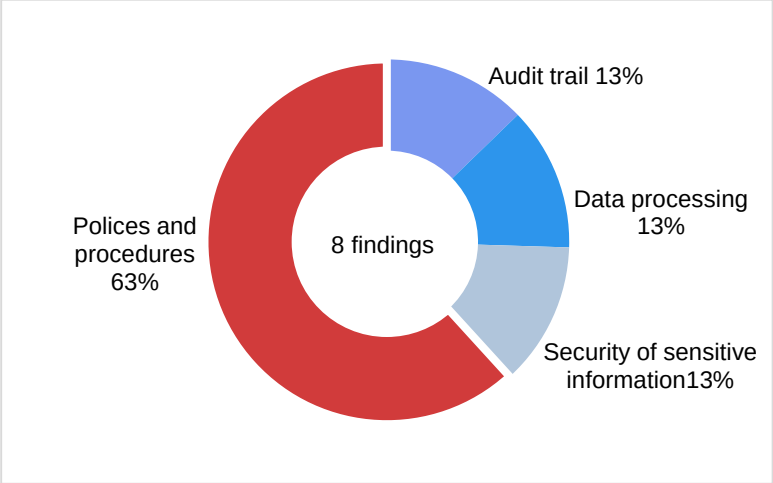
    a. **Appropriately control sensitive electronic information. These controls should ensure that the information is appropriately stored and access is restricted to authorised users only. As part of an overall information security strategy, DCS should implement good access control practices that include all users and roles.**

Response from the Department of Corrective Services

The Department of Corrective Services welcomes the application controls review by the Office of the Auditor General. The Department notes that overall the Total Offender Management System was found to meet the needs of the Department's staff to manage offenders in correctional facilities and the community. The Department thanks the Office of the Auditor General for its advice and recommendations on how it can continue to review and improve its systems and processes.

The Department accepts the recommendations and notes that a number of findings have been addressed by the Department prior to the completion of this audit. The Department is acting on all remaining recommendations as a matter of priority and is committed to the continued improvement of its information systems.

Controlled Waste Tracking System – Department of Environment Regulation



Background

Controlled waste is defined under the *Environmental Protection (Controlled Waste) Regulations 2004*. It includes substances like acids, arsenic, asbestos, clinical waste, heavy metals, organic compounds, tyres, sewage, food processing and grease trap wastes and waste pharmaceuticals and medicines. The overarching aim of the regulations is to minimise the risk to the public and the environment of inappropriate or illegal transport and disposal of controlled waste.

The Department of Environment Regulation (DER) is responsible for monitoring and controlling the transport of controlled waste in Western Australia. Transportation of controlled waste is divided into 2 categories: bulk and packaged. Bulk controlled waste is liquid and is transported in a dedicated tank. Packaged controlled waste refers to waste that is transported loose, for example, tyres and soil, or waste in containers like drums and skip bins. The regulatory requirements differ between bulk and packaged waste.

Under the regulations, controlled waste carriers must be licensed. Any drivers who transport bulk controlled waste, and the vehicle and tanks they use, require additional licences. Facilities that receive controlled waste, known as waste facilities, must be registered with DER. Businesses that generate or possess controlled waste can only use licensed carriers to collect and transport waste for disposal.

Licensed carriers are required to record transported waste using individually numbered controlled waste tracking forms. DER issues these forms either electronically, or in a hard copy book. Carriers must use the forms for any movement of bulk controlled waste, or if they are transporting 200kg or 200L or more of packaged waste. The waste carrier and the facility receiving the waste must each lodge a copy of the tracking form with DER. Required details in the form range from the licence of the carrier to the amount and type of waste transported or received.

DER's Controlled Waste Tracking System (CWTS) analyses the details contained in the forms and triggers alerts if it detects inconsistencies with a condition of licence or mismatches between the data submitted by the carrier and the waste facility.

The CWTS records the licence details of the 440 controlled waste carriers and lists 370 disposal facilities. Between 90,000 and 100,000 transport events move about 925,000 tonnes of liquid controlled waste each year.

Conclusion

The CWTS is fit for purpose. However, DER makes no adjustments for thousands of flagged data entry discrepancies thereby rendering the information on amounts and types of controlled waste unreliable. Unreliable information makes it difficult for DER to monitor compliance and to target its compliance and enforcement activities at areas of highest risk.

A range of weaknesses with the management of CWTS puts the data integrity and continuity of operation at unnecessary risk. These include excessive numbers of staff with administrator access and a lack of agreement between the CWTS software developer and the state agency that runs the IT infrastructure regarding roles and responsibilities.

Audit Findings

Uncorrected data errors result in unreliable information and poorly targeted compliance effort

DER does not consistently investigate or correct data discrepancies or entry errors in CWTS. As a result, DER is unable to rely on the data for monitoring compliance by controlled waste disposal facilities and carriers.

DER tracks waste transportation using a controlled waste tracking form that contains information on:

- type and amount of controlled waste
- date and time when it was picked up
- date and time delivered to the waste facility
- the driver's licence number
- the vehicle registration number and/or waste tank used to carry the waste.

The CWTS generates an alert when mismatches occur between the tracking form lodged by the carrier and the form lodged by the waste facility that takes delivery of the waste as well as mismatches with licence conditions.

The system generated around 20,000 alerts from the approximately 100,000 transport events that occurred in 2015.

Mismatches can relate to procedural issues, such as drivers or the waste facility not completing the tracking form within 14 days of the waste being unloaded, or the driver not having a valid controlled waste licence or a vehicle or tank not licensed to carry the type of waste collected. However, they can also be of potentially more serious matter.

About 20% of mismatches (4% of transport events) are between the type or amount of controlled waste unloaded by a waste carrier and that received by the waste facility. These are arguably high-risk alerts as they potentially indicate incorrect disposal of controlled waste and harm to the environment and public health.

However, DER advised us that preliminary analysis it did in 2015 showed that about 81% of alerts were due to data entry errors.

Nevertheless, we expected that when alerts occur, DER would establish the reason for the mismatch. If due to a data entry error, then it would be corrected and if due to some other reason, then it would be investigated. Analysis of alert data could also identify carriers and waste facilities that repeatedly input incorrect information. Repeated under reporting of waste amounts by waste facilities could indicate an attempt to avoid exceeding licence conditions.

However, DER does only limited follow-up of individual alerts, resulting in data errors remaining in the system and investigations of potentially incorrect disposals not occurring.

Instead, it focuses its effort and resources on attempting to process alerts and prioritise and select those alerts it will follow-up. DER analyses the data in the CWTS and produces a quarterly management report of unusual trends, or more significant high-risk data mismatches. This quarterly report informs DER's compliance follow-up work.

However, the uncorrected errors in the CWTS are so extensive that these reports carry a warning that the data should not be relied on. The effect in one case that we reviewed was DER investigating waste facilities suspected of exceeding their licensed controlled waste amounts only to find the data was wrong.

Effective operation, development and maintenance of CWTS is at greater risk because of a lack of formal arrangements with service providers

CWTS is vendor-developed software. The vendor is responsible for maintenance and changes to the CWTS application.

However, there is no contract between DER and the vendor. Without a contract, roles, responsibilities and remuneration for services are potentially open to negotiation or dispute. It also places at risk DER's ability to manage effectively its ongoing development and maintenance of the CWTS.

DER also has no formal agreement between itself and another state government agency that manages the IT infrastructure (servers, network, supporting software) that runs the CWTS.

As a result, key IT management processes are not defined or agreed, including roles and responsibilities for system security, priorities for system recovery in the event of a disaster, backup of data, and management of changes to the system. Without these formal obligations in place, DER may find that it cannot quickly recover CWTS in the event of a disruption or incident.

High numbers of people with administrator access puts data integrity at risk

DER does not have any formalised policies in place that govern the management and use of CWTS. Policies help ensure that roles, responsibility, conditions of use, and system management are understood. We identified the following issues relating to DER's management of CWTS users and activities:

- 24 DER staff members, or 40% of all internal users, have administrator level access to the CWTS. Administrator access gives users the ability to edit or delete waste tracking events and associated data. Administrators can also create, modify, and remove other user accounts. Having several users with this level of privileged access increases the risk that data may be wrongly changed or deleted.
- DER does not periodically review who has access to the system and if their level of access is appropriate. These reviews ensure that any person that has left DER has their account removed and that the level of access for persons whose role has changed remains appropriate.
- The system logs actions and changes made by all users, including administrators. However, these logs are not reviewed to ensure administrator and other actions are appropriate. Without this review, any unauthorised changes or access to sensitive information may go undetected.
- While CWTS allows all administrator user accounts to read system logs, not all users have the in-depth technical knowledge to access the logs. CWTS does not have an

easy to use logging interface that contains all user actions. Logs are disparate; they are stored in different areas of the application and underlying database. As a result, DER must rely on the software vendor to support any investigations that require analysis of the logs. The same contractors also have the ability to delete or modify these logs. DER may be unable to rely on or access logging data if there is a dispute with the contractor. It would also not be able to identify inappropriate changes to the logs or link these to the relevant user.

Recommendations

1. **By August 2016, the Department of Environment Regulation should:**
   a. **Establish appropriate formal agreements with relevant service providers for the CWTS.**
2. **By June 2017, the Department of Environment Regulation should:**
   a. **establish a process to regularly review and correct mismatched data**
   b. **develop and implement supporting policies and procedures for the CWTS including: management and review of user accounts and access privileges; and management and review of system logs.**

Response from the Department of Environment Regulation

The Department of Environment Regulation fully accepts Recommendation 1.

Management fully accept the responsibility to implement a contract between DER and any successful tenderer with respect to the services currently being provided by the current vendor.

The Department of Environment Regulation accepts, in part, Recommendation 2.

Analysis will be undertaken of the system to identify mismatch system warnings, using Corporate Policy Statement No 7 – Operational Risk Management, to identify the warnings that may indicate a potential risk to the environment or public health.

An operational procedure may be prepared, documenting the procedure for the routine review and investigation of the identified mismatch system warnings by appropriate Controlled Waste staff.

Analysis of the current DER CWTS users against their DER role has commenced. This will clarify the access permissions required for role-based access control of the CWTS. The system will be reviewed ensuring the required changes can be made and whether the system source coding can be amended. If so, new role-based user access profiles will be applied to the system and across each current DER user account.

An operational procedure will be prepared, documenting the procedure for the routine reviews of the current user access profiles.

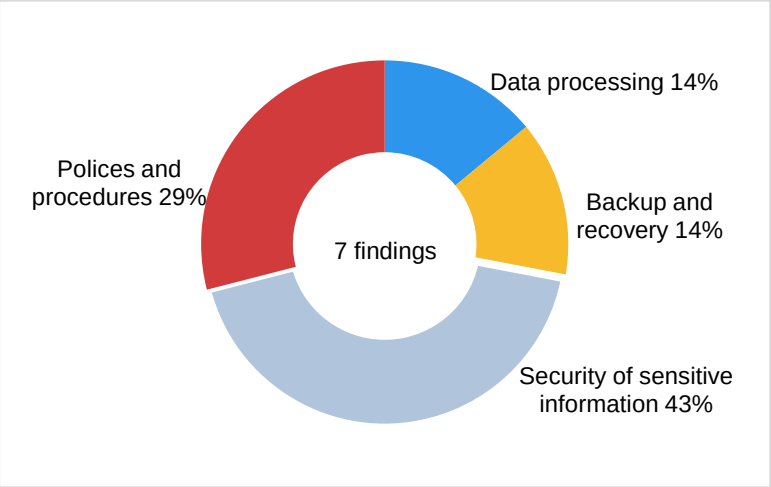
Analysis will be undertaken of the system audit logs, based on the administrator privilege actions, to identify the issues at high risk from potential malicious behaviour.

A review of the system will determine if:

- the required changes can be made; and
- resources are available to develop a system audit log report that will display those actions deemed a high risk.

If so, an operational procedure will be prepared, documenting the procedure for routine review and investigation of the audit log report by appropriate Controlled Waste staff.

Treasury System – Gold Corporation



Background

Gold Corporation (the Corporation) was created by the *Gold Corporation Act 1987* to take over the operations of the Perth Mint. The Corporation operates Australia's largest precious metals refinery. Most of the gold mined in Australia and some from neighbouring countries is refined at its Western Australian facility.

Activities of the Corporation and its subsidiaries include refining precious metals, the manufacture of coins and bars, the supply of precious metal blanks and storage and safekeeping services for precious metals. It also designs and markets Australia's official bullion coin program.

The Corporation uses an in-house developed application, Treasury System (TS) to manage precious metal transfers, trades, metal swaps, shipments and consignments and over 1,000 clients from Australia and overseas. Clients are mainly mining companies and bullion banks. On average, over 200,000 ounces of gold with an approximate value of $344 million and over 400,000 ounces of silver valued at $9.2 million are traded via TS on a weekly basis[1].

Conclusion

Overall TS is a well-functioning application that assists the Corporation to manage its precious metal trading effectively. The system also provides useful information and reports.

However, improvements can be made to the documentation of information and communications technology risks, security over back-up tapes, software updates and disaster recovery testing.

[1] These values were at May 2016.

Audit findings

Information risk management

Gold Corporation has extensive prudential management policies that incorporate financial and treasury risks.

However, the extent to which information and security risks are integrated into the policies is unclear as the risk assessment processes are not documented – though staff advised that they were considered.

Good documentation is an important means of ensuring that the Board and senior management have visibility and a good understanding of the information and security risks affecting the Corporation. Good documentation also helps facilitate risk reviews and to ensure that risk treatment remains appropriate.

Security of sensitive data could be improved

The TS stores financial and personal information of customers, both Australian and international, business and individual. The Corporation is not adequately managing some of the risks associated with information and software updates for key systems:

- **Backups not encrypted** – 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 misplaced or stolen. If encrypted, then the data would be inaccessible to anyone that did not possess the decryption keys. Encryption of backup media where confidentiality is important is in accordance with the international standard for information security (ISO27002/2013).
- **Basic security updates not applied** – software updates released by vendors to fix known security vulnerabilities were not applied to all key servers. Without these updates, attackers could exploit known vulnerabilities and may gain access to systems and information. An effective 'patching' process that keeps software up-to-date is vital to protect against cyber threats and data loss.
- **Vulnerability assessments are not conducted** – the Corporation does not perform vulnerability assessments across their IT systems and therefore cannot give assurance that its software updates are applied correctly and are not vulnerable to threats. Ideally vulnerability scans should be performed every month. Regular scanning ensures new vulnerabilities are detected in a timely manner.
- **Unsupported operating systems** – servers run operating systems that the vendor no longer supports or provides security updates, thereby increasing the risk of the IT systems and information being compromised.

Controls to ensure ongoing operations

The Corporation has concluded that disruptions to the TS of more than two hours can impact its day-to-day operations and may result in financial loss or reputational damage.

The Corporation has developed an IT disaster recovery plan to restore services in the event of an outage. Although it tested the plan in 2011, the testing was limited and therefore not reliable. Good testing involves various scenarios to help ensure it is well designed and reliable.

The Corporation recognised this issue in 2014 and is now developing a testing program and planning a controlled failover test of key systems in 2016. A controlled failover test assesses whether systems can be completely restored.

Access control policy and procedures

We found that the Corporation did not have a documented access control policy and relevant supporting procedures for TS. We also identified that a high privilege administrator account for TS has been configured with no password expiry. During the audit, the Corporation drafted a new account management policy to address these issues, which includes access to TS.

Without appropriate policy and procedures over user access to systems and networks, there is an increased risk of unauthorised or inappropriate access.

Manual reconciliations

The Corporation's settlement team performs manual reconciliations for cash settled transactions processed by the TS. Most transactions are either metal swaps or settled by crediting the Corporation's London Credit Account. For the period we tested, an average of 26 transactions per day were cash settled. After transactions are entered into TS, the settlement team document these transactions manually in a spreadsheet that reconciles the cash transactions with the banking information.

Although manual data processing is generally less accurate and efficient than automated processes, the Corporation advised that these processes have proven effective. The Corporation also advised that current system limitations mean that these controls cannot be automated.

Recommendations

1. **By August 2016 the Gold Corporation should:**
    a. **integrate its information risk management process with that of the business, in line with better practice**
    b. **ensure that appropriate controls are in place to protect information at all times including data stored on backups**
    c. **identify and apply updates within a timely manner to IT infrastructure. The Corporation should also conduct regular internal vulnerability scans**
    d. **improve the disaster recovery environment to minimise the risk of system outages and conduct adequate disaster recovery testing on a regular basis.**
2. **When it next updates or reviews its systems, the Corporation should consider automating the reconciliation of cash settled transactions.**

Response from the Gold Corporation

Integrate its information risk management process with that of the business, in line with better practice

The Corporation accepts this finding and has included the risks outlined in the IT risk register for on-going pro-active monitoring and management.

Ensure that appropriate controls are in place to protect information at all times included data stored on backups

The Corporation accepts that it is important to have in place appropriate controls to protect information at all times, including data stored on backups and takes the security of sensitive information seriously. The Corporation has completed a further comprehensive risk assessment to satisfy itself as to the appropriateness of the controls surrounding such data. This included an assessment of the physical security controls implemented at the vaulted storage facility and an assessment of the operational processes and procedures embedded within the facility and transportation methods. The controls were found to be appropriately designed to mitigate risk and are operating effectively. The Corporation has satisfied itself on the design and operating effectiveness of the current control structure, however the Corporation accepts that this issue needs to be actively monitored and managed and also accepts that its current procedure may need to change based on future assessments.

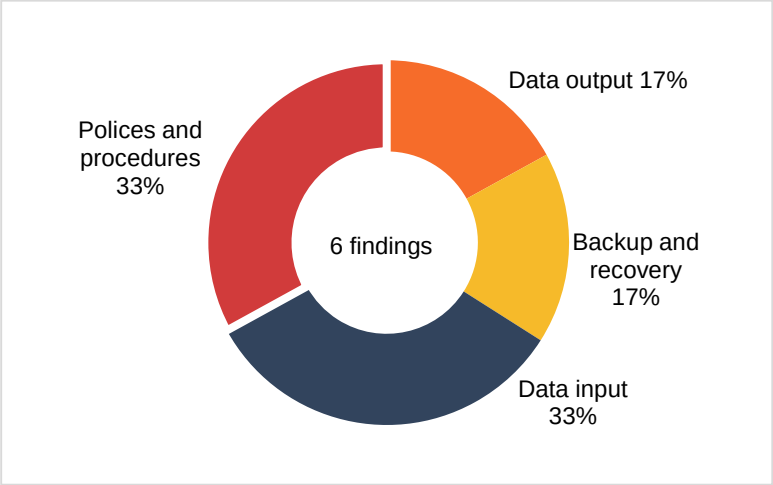
Identify and apply updates within a timely manner to IT infrastructure. The Corporation should also conduct regular internal vulnerability scans

The Corporation accepts the need to apply security updates to its applications and systems within an appropriate and timely manner. The Corporation also accepts that regular testing for security vulnerabilities is an effective way to identify and mitigate against potential threats. Monthly security updates are now applied to all servers across the organisation in line with current policy and vulnerability scans are planned to commence later in the year.

Improve the Disaster Recovery environment to minimize the risk of system outages and conduct adequate DR testing on a regular basis

The Corporation accepts the need to regularly test the disaster recovery environment. A successful failover of all key systems including those referred to in the Summary of Findings has been completed with no issues identified. As part of the failover from the production environment to the disaster recovery environment the Corporation successfully ran all its production systems from the disaster recovery environment for 7 days without issue to business continuity. The Corporation plans to ensure regular testing occurs using a variety of possible failure scenarios.

SmartParker – Public Transport Authority



Background

The Public Transport Authority (PTA) manages around 21,000 parking bays at 51 train stations in Western Australia using the SmartParker system. The system has been in use since July 2014 after it was purchased from and customised by a third party vendor. The vendor continues to provide ongoing support for the system.

The system allows the public to use their public transport card (SmartRider) to 'tag on' to pay the $2 fee for parking in PTA carparks. The fee is deducted from their SmartRider balance. The fee, which is charged on weekdays only, provides validated parking for 24 hours. It applies to all vehicles including motorbikes and motorised scooters. PTA parking revenue in 2014-15 was $7.97 million. Over 80% of parking revenue is collected by SmartParker.

To use SmartParker, the public must link their vehicle licence plate to their SmartRider either by using the 'My Account' page on the Transperth website or by contacting the Transperth call centre. A maximum of 3 vehicles can be registered to a single SmartRider, but only 1 vehicle can be marked as 'active' at any time. This is the vehicle that will be parked at a train station that day. When using another vehicle, the public need to ensure that they have changed their active vehicle before tagging on.

Conclusion

Overall, SmartParker is an effective system for managing parking in PTA carparks. However, control weaknesses in data validation and supporting processes could result in the issuance of parking fines that the public will consider unwarranted or unfair. Although fines can be appealed, incorrectly issued fines can damage public confidence and are time consuming for the public and PTA.

The obligations of the PTA and its service provider, in the event of an incident that may disrupt the system, are unclear as the parties have not formally documented or set these out in a contract.

The PTA has not created disaster recovery plans for SmartParker. These plans are required to minimise disruption to the system in the event of a serious incident or disaster. Important day-to-day SmartParker processes have also not been documented. This includes procedure manuals for electronic checks of meter performance, gathering and reporting of systems statistics and user management tasks.

PTA has previously identified many of the issues in this report and is working towards improved reporting, number plate validation and more efficient processing of infringements.

Audit findings

System process and data validation weaknesses undermine confidence

The SmartParker system is associated with the issuing of a large number of parking infringements, many of which the PTA later cancels.

Effective use of the SmartParker system is dependent on users:

- ensuring they link their vehicle (or vehicles) licence plate numbers to their smart card
- ensuring the licence plate number they link is correct
- ensuring before they tag on the vehicle they will park that day is selected. The system works on a default basis. It will assume that the parked vehicle is the same used on the previous occasion, unless told one of the other authorised vehicles is parked.

A failure in one of the above steps followed by the checking of the vehicle by a parking inspector will result in the issuing of a parking infringement. While prevention of these errors rests first and foremost with the public, the PTA has a responsibility to contribute to prevention through good communication and system processes.

Parking inspectors use a smart phone with a custom number plate recognition application. This software uses the device's camera to 'read' number plates. If a plate is not associated with a SmartRider that has tagged on in that car park, on that day, it will generate an alert and the issuing of an infringement notice.

We sampled one day of parking data and found that of the 15,726 persons who tagged on to park, 143 did not have a vehicle registered to their SmartRider account. In our view, this is a serious system weakness.

The PTA recognises that the types of errors described above are major contributors to the high number of infringements issued each day. Typically, the PTA issues about 200 parking infringements per day. The public can appeal parking infringements and the PTA will cancel the infringements if satisfied that the appellant made an effort to use the system correctly. The PTA advised that it cancels about 40% of the parking infringements it issues. The PTA's infringement systems cannot easily report on how many appeals related to SmartParker.

However, the appeals process is time consuming for the appellant, costly for the PTA and is damaging to the public's satisfaction with public transport.

The PTA has advised that it will investigate the feasibility of linking SmartParker with Department of Transport systems to ensure that correct licence plate numbers are entered. We welcome this move but note that it will not solve the issue of people not registering vehicles to SmartParker.

Manual processes increase the risk of errors in infringement notices

The PTA's processing of about 200 parking infringements per day requires a large amount of manual data entry and processing. Staff record details of an infringement in 3 different locations:

- the parking inspector's mobile device, which identifies infringing vehicles by reading the numberplate and comparing it to SmartParker records

- a hand written paper ticket which is left on the vehicle, with 2 carbon copies retained by PTA
- infringement details from the carbon copy tickets are then entered manually into the enforcement system the following day.

Parking inspectors at train stations will compile ticket copies and transport them to the central enforcement office for processing. Copies of tickets could be lost or damaged during this manual handling. An enforcement officer processing paper tickets may incorrectly issue or withdraw a fine if a paper ticket is misinterpreted.

These manual processes are inefficient and potentially unreliable. The PTA could automate these tasks. Electronic alternatives are readily available and will provide efficiency gains and added confidence in the ticketing process.

Management reporting requires system improvements

We found that PTA does not have an efficient process for producing management level reports of SmartParker enforcement and carpark usage. Although the system generates some generic reports, these are not meeting management's needs. Staff use spreadsheets to create daily statistics and trends on parking bay use. This information is then used to create daily and monthly management reports on parking activity.

The manual compilation of reports is inefficient and increases the risk of input errors, affecting the reliability of reporting and of management making incorrect decisions.

Individual business areas create and tailor reports for their needs. However, these are not made available to other business areas, as PTA does not collate the information into a central repository to allow automated and flexible reporting. Without a centralised view of the parking data, PTA does not have visibility of its overall performance. This may impact its ability to make decisions affecting the long term improvement of SmartParker.

The PTA is currently reviewing its reporting processes and plans to automate reports where possible.

Controls to ensure ongoing operations could be strengthened

The PTA has identified SmartParker as critical to day-to-day operations. An outage of the SmartParker system could result in a loss of revenue, as well as delay the processing of infringements. We found weaknesses in the following areas that may delay full restoration of operations following an incident:

- the PTA and its service provider do not have a formal agreement that defines the obligations of each party and the services to be provided. In the event of an incident, PTA may be unable to rely on the service provider to support SmartParker in timely manner
- there is no disaster recovery plan for SmartParker. Disaster recovery plans assist by describing how to recover IT systems in the event of an incident that causes an outage or disruption to services
- the PTA has not documented some important daily SmartParker tasks. For instance, formal procedures for checking the state of the parking meters, entry of infringement data and managing users within SmartParker. The PTA relies on the knowledge of their current staff to ensure these tasks are completed consistently and correctly. Formalising the procedures could enable the PTA to continue operation even when staff with the knowledge of the operations are unavailable.

Recommendations

1. **By August 2016 the Public Transport Authority should:**
   a. **establish a formal contract and service level agreement with SmartParker's service provider**
   b. **develop and test disaster recovery plans for the system and supporting infrastructure**
   c. **document important SmartParker tasks, detailing the requirements and step by step procedures. These documents should be stored to allow access by suitable staff and be reviewed and updated periodically.**
2. **By December 2016 the Public Transport Authority should:**
   a. **collaborate with other agencies and organisations to ensure that licence plates recorded in SmartParker can be validated**
   b. **identify opportunities to reduce duplicate data entry and streamline the parking Infringement process**
   c. **enhance reporting capabilities to automate common reports and provide easy access to create ad-hoc reports across parking and infringement operations.**

Response from the Public Transport Authority

The findings and recommendations of the OAG SmartParker report are acknowledged by the PTA. It should be noted that the contract with the service provider is now ready for finalisation and the other report findings will be considered/addressed as the PTA seeks to implement the next generation of parking technology which will involve back office validation, issuing and processing of parking infringements.

General computer controls and capability assessments

General computer controls and capability assessments

Conclusion

We reported 454 general computer controls (GCC) issues to the 45 agencies audited in 2015 compared with 398 issues at 42 agencies in 2014.

Only 10 agencies met our expectations for managing their environments effectively, compared with 11 in 2014. More than half of the agencies are not meeting our benchmark expectations in 3 or more categories and the overall result showed a 3% decline on the prior year.

Change controls and physical security are managed effectively by most agencies, but the management of IT risks, information security, business continuity and IT operations need a much greater focus.

Background

The objective of our GCC audits is to determine whether the 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 2015 we focused on the following control categories:

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

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.

What did we do?

We conducted GCC audits and capability assessments at 45 agencies. This is the eighth year we have assessed agencies against globally recognised good practice.

We provided the 45 selected agencies with capability assessment forms 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[2] 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.

0 (non-existent)	Management processes are not applied at all. Complete lack of any recognisable processes.
1 (initial/ad hoc)	Processes are adhoc 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

What did we find?

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 45 agencies we audited. We expect agencies to rate a level 3 or better across all the categories.

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

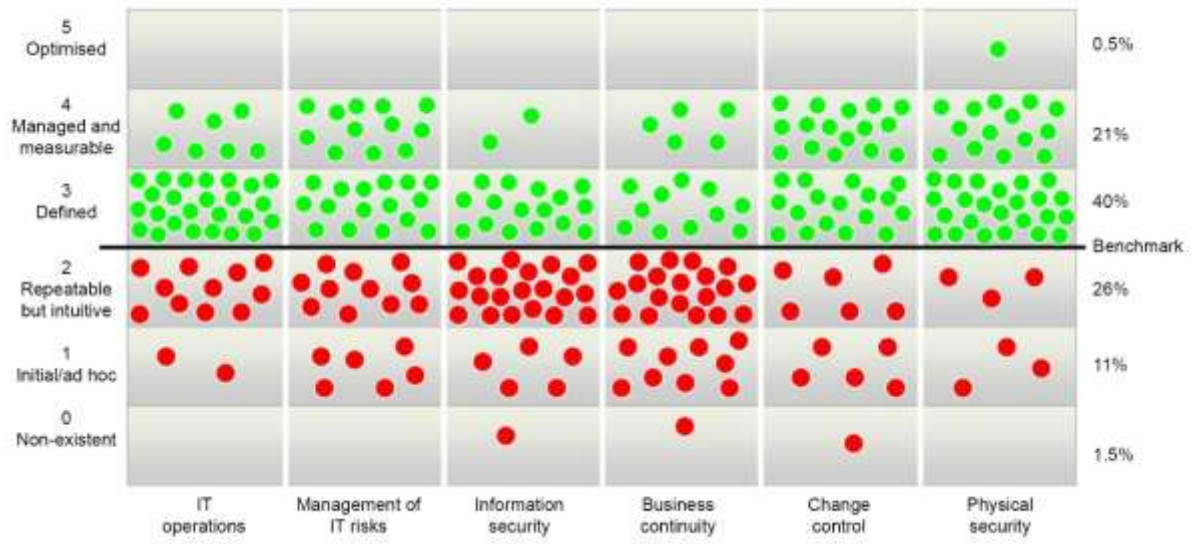


Figure 1: Capability maturity model assessment results

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	2014 %		2015 %
IT operations	74	↓	71
Management of IT risks	60	↑	64
Information security	38	↑	40
Business continuity	45	↓	36
Change control	76	↓	73
Physical security	90	↓	87

Table 2: Percentage of agencies at level 3 or above

The 2015 results were disappointing with a 3% average decline across all areas when compared with 2014. Results in the level 3 to level 5 categories fell to 61.5% compared to 69% in the previous year. However, this figure in 2012 was 53%, which demonstrates a general improvement over 3 years.

Ten of the 45 agencies were level 3 or above across all categories in 2015 compared to 11 in 2014. Thirty-four agencies were able to achieve level 3 or higher in at least 3 categories compared to only 14 agencies in 2014.

Nine agencies made improvements in at least 1 category without regressing in any other category. Thirteen agencies showed no change. Nine agencies moved up 1 category but went down in another. Eight agencies regressed in at least 1 category without making any improvements.

IT operations

The rating for 'performance in IT practices and the service level performance provided to meet their agency's business' fell 3% in 2015 compared to the previous year. However, there has been overall improvement of 23% 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:

- 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.

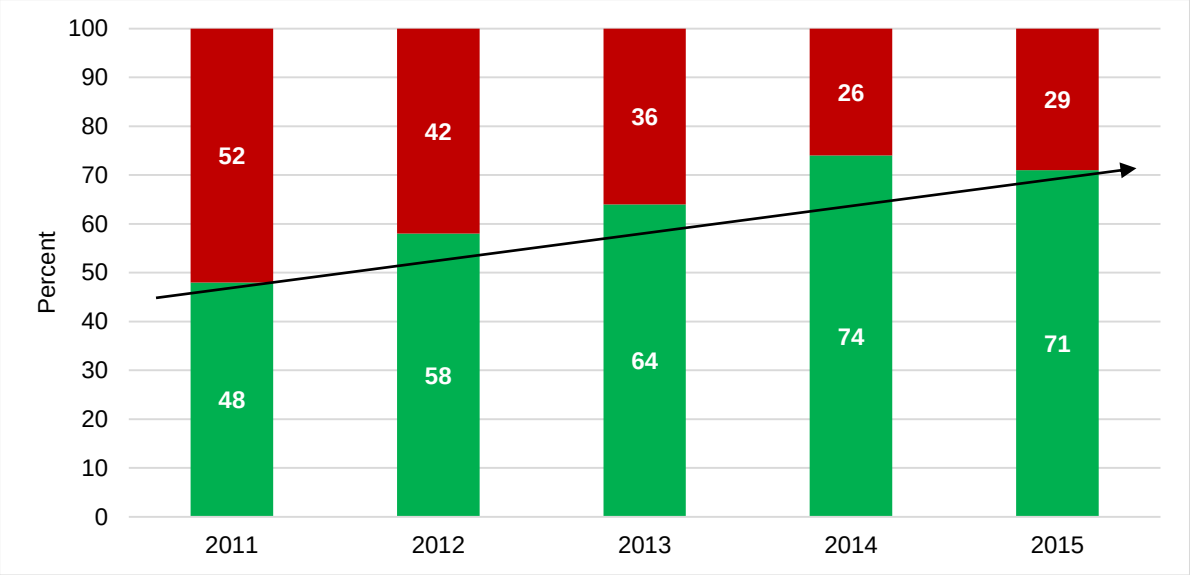


Figure 2: IT operations

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 and communication technology strategies not in place
- no logging of user access and activity to critical systems or sensitive data
- network logs 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, changes to databases with confidential information

- no follow-ups to automated alerts from security devices and applications
- several agencies are running unsupported operating systems
- no user education of security policy and security related responsibilities and induction processes not implemented or followed
- unsupported databases for critical systems
- background checks for key staff not undertaken
- no incident management procedure
- sensitive information stored in excel spreadsheets and widely accessible
- 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.

Management of IT risks

Sixty-four percent of agencies met our expectations for managing IT risks a 28% improvement since the first assessment in 2008, with agencies showing improved management controls over risks.

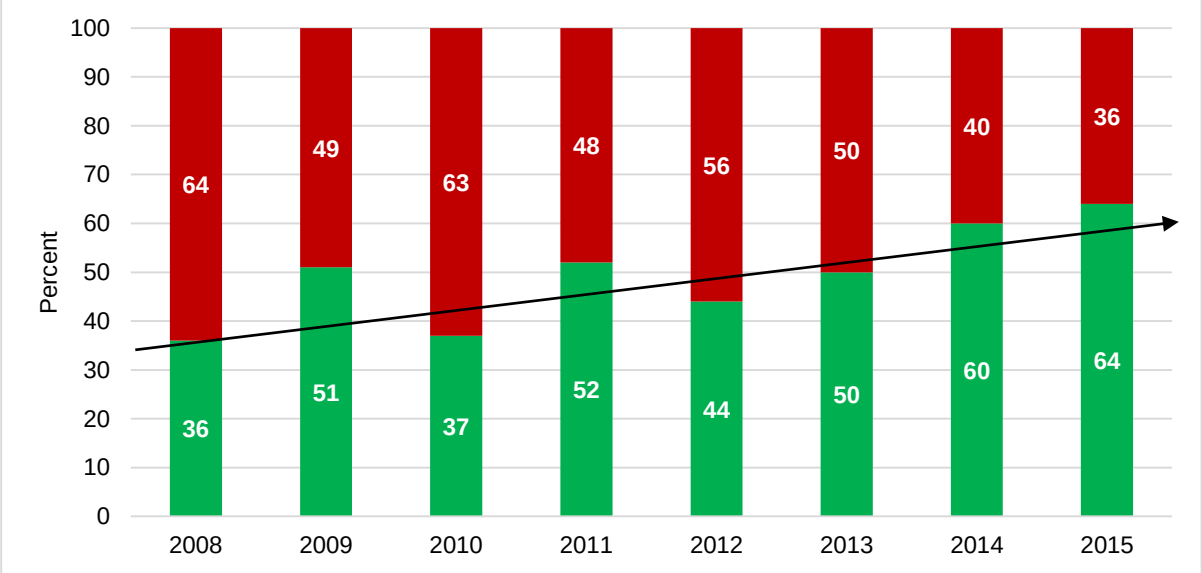


Figure 3: Management of IT risks

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 established 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.

Information security

Only 40% of agencies met our benchmark for effectively managing information security, up 2% 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 8 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.

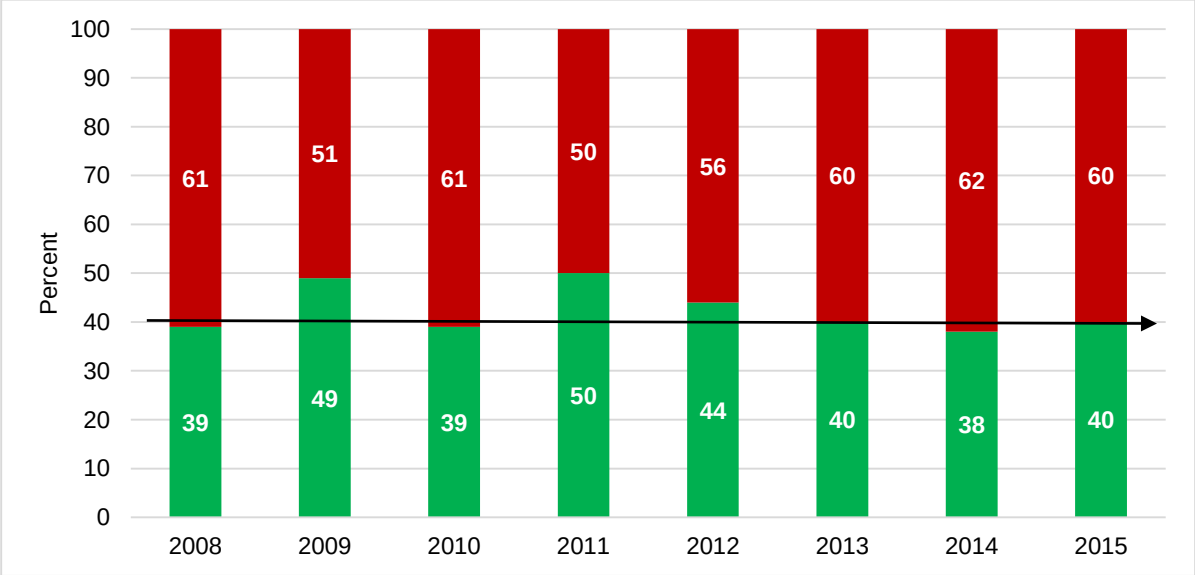


Figure 4: Information security

Weaknesses we found included:

- information security policies did not exist, were out of date or not approved
- easy to guess passwords for networks, applications and databases, e.g. *Password1, guest*
- applications without critical patches applied (1,000's critical and high severity)
- operating systems missing critical patches (1,000's critical and high severity)
- highly privileged generic accounts shared with many staff and contractors, some accounts exist without agency knowledge
- lack of processes to identify security vulnerabilities within IT infrastructure
- no review of application and network accounts

- weak password controls such as complexity, length, history, expiry, lock out
- firewalls and intrusion detection/prevention systems not configured correctly leaving exposures
- unknown accounts accessing firewalls and accounts using insecure access methods
- not installed or out of date anti-virus software
- default database accounts remain unchanged with credentials widely known and published on the internet
- terminated staff used remote access accounts
- unauthorised software installations on servers and staff computers
- local administrator privileges granted to allow any activity.

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

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 64% of the agencies still not having adequate business continuity and disaster recovery arrangements in place. The trend over the last 8 years has shown no notable improvement. This may mean that agencies do not afford this proper priority.

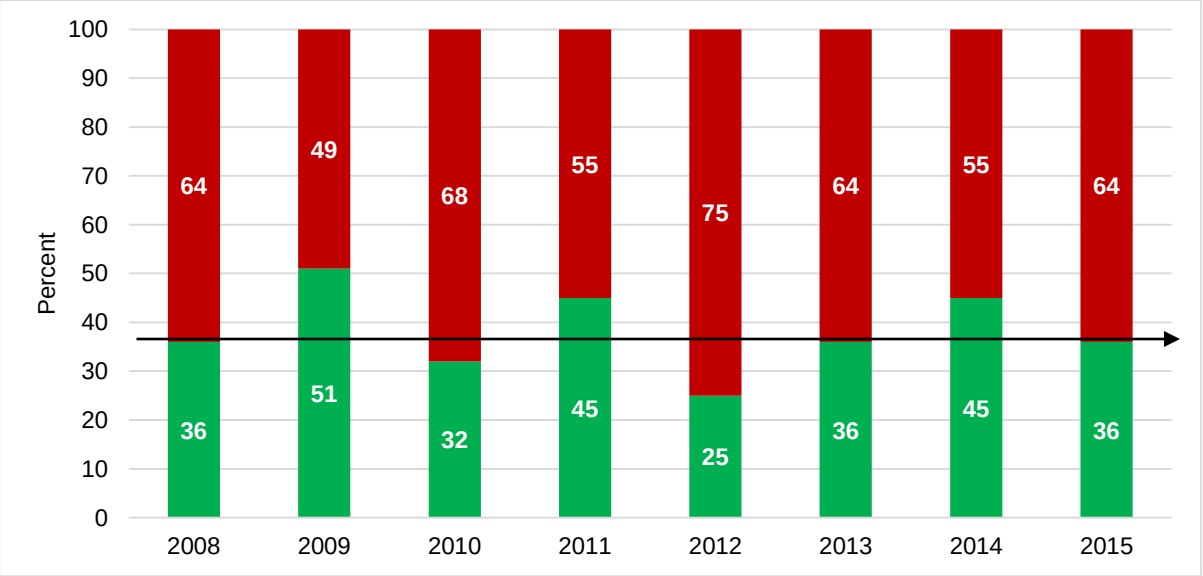


Figure 5: Business continuity

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.

Change control

We examined whether 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 almost 3 in 4 agencies achieving a level 3 or higher rating.

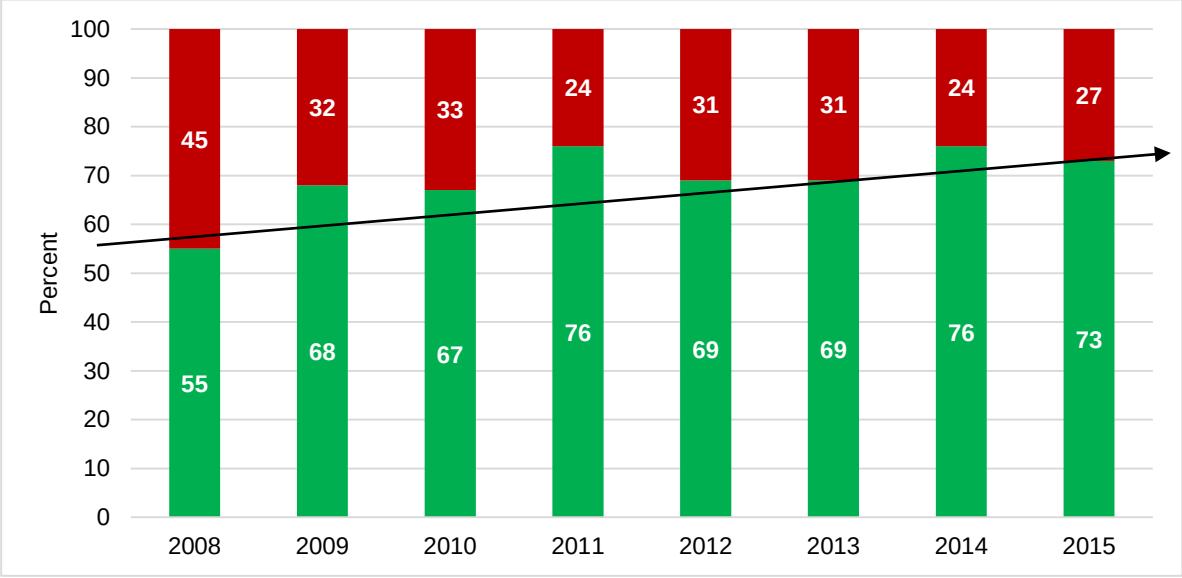


Figure 6: Change control

Weaknesses we observed included:

- no formal 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 agency's 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 45 agencies fell below our expectations for the management of physical security.

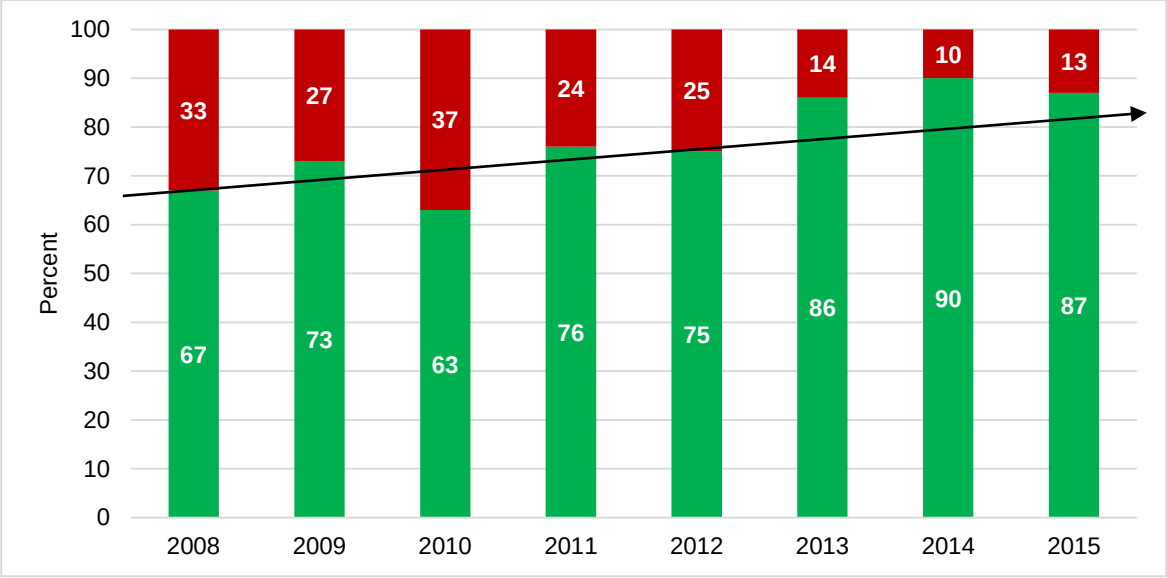


Figure 7: Physical security

Weaknesses we observed included:

- power generators in the event of power failure not tested
- no fire suppression system installed within 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 8 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.

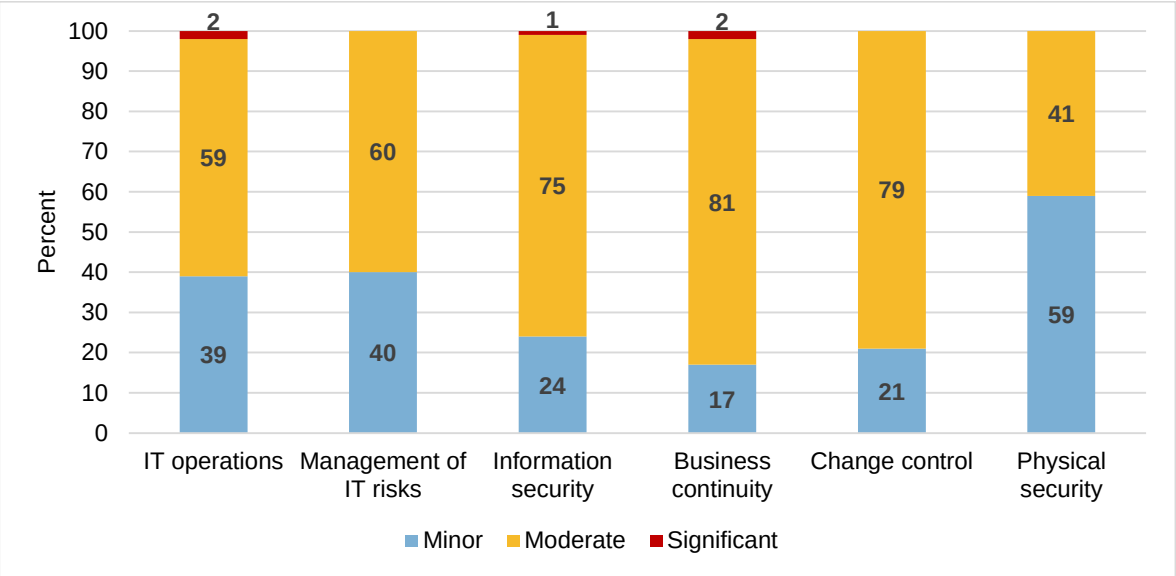


Figure 8: Distribution of ratings for the findings in each area we reviewed

Recommendations

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.

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.

Information security

Agencies should ensure good security practices are implemented, up-to-date and regularly tested and enforced for key computer systems. Agencies must conduct ongoing reviews for 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.

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 No.	Reports 2016	Date Tabled
10	Opinions on Ministerial Notification	8 June 2016
9	Payment of Construction Subcontractors – Perth Children's Hospital	8 June 2016
8	Delivering Services Online	25 May 2016
7	Fitting and Maintaining Safety Devices in Public Housing – Follow-up	11 May 2016
6	Audit of Payroll and other Expenditure using Data Analytic Procedures	10 May 2016
5	Audit Results Report – Annual 2015 Financial Audits – Universities and state training providers – Other audits completed since 1 November 2015; and Opinion on Ministerial Notification	10 May 2016
4	Land Asset Sales Program	6 April 2016
3	Management of Government Concessions	16 March 2016
2	Consumable Stock Management in Hospitals	24 February 2016
1	Supplementary report Health Department's Procurement and Management of its Centralised Computing Services Contract	8 June 2016 17 February 2016

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