Western Australian Auditor General's Report

Information Systems Audit Report

Report 11 – June 2013

VISION
of the
Office of the
Auditor General

Excellence in auditing for the benefit of Western Australians

MISSION
of the
Office of the
Auditor General

To improve public sector performance and accountability by reporting independently to Parliament

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 persons with hearing and voice impairment)

On request this report may be made available in an alternative format for those with visual impairment.

ISBN: 978-1-922015-24-2

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Information Systems Audit Report

Report 11
June 2013

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

INFORMATION SYSTEMS AUDIT REPORT

I submit to Parliament my *Information Systems Audit Report* under the provisions of sections 24 and 25 of the *Auditor General Act 2006*.

COLIN MURPHY
AUDITOR GENERAL
27 June 2013

Contents

Auditor General's Overview

The *Information Systems Audit Report* is tabled each year by my Office. This report summarises the results of the 2012 annual cycle of audits, plus other audit work completed by our Information Systems group since last year's report of June 2012. This year the report contains three items:

- Information Systems – Security Gap Analysis
- Application controls audits
- General computer controls and capability assessments of agencies

In the first item we benchmarked 21 agencies against the International Standard for Information Security – ISO 27002. The standard sets out controls for ensuring computer systems are designed, configured and managed to preserve the confidentiality, integrity and availability of information. Most of these controls are recognised as good practice and require minimal effort to implement. Our information systems audits consistently highlight a need for agencies to pay greater attention to the security of their information systems. Therefore it was not surprising to find the majority of agencies we looked at had significant gaps when assessed against these standards. The standards provide useful guidance to agencies on how to take a systematic approach to identifying and addressing these gaps. While the international standards for information security are not mandatory in Western Australia, I urge agencies to seriously consider them.

The second item reports on the audit of five key business applications at four agencies. Most of the applications we reviewed were working effectively. However, we identified a number of serious weaknesses with the Firearms Management System managed by Western Australia Police (WAP). Because of these weaknesses WAP lacks reliable information to effectively manage licensing and regulation of firearms in Western Australia.

The final item presents the results of our general computer controls and capability assessments of agencies. Only three of the 36 agencies we assessed were rated as having mature general computer control environments across all six categories of our assessment. Half the agencies failed to meet our expectations for three or more of these categories.

Information Systems – Security Gap Analysis

Conclusion

Ninety per cent of the agencies we reviewed had serious gaps in their management of information security when assessed against better practice international standards. Many of the agencies sampled are not adopting a strategic approach to identifying and assessing risks. In the absence of a strategic approach agencies may be wasting resources on areas of minimal risk while leaving critical areas exposed.

This result suggests a lack of understanding and implementation of good information security practices across the Public Sector and of systems being put at unnecessary risk.

Background

Information security is the protection of information from a wide range of threats in order to ensure business continuity and minimise a range of business risks. Essentially it is the preservation of confidentiality, integrity and availability of information. This is particularly important with the increase in interconnected computing environments and ever increasing threats.

Our annual general computer controls (GCC) audits provide insight into agencies' information systems (IS) security. Although the main objective and scope of these audits is supporting financial audits, we consistently report significant information security issues. This year we found over 92 per cent of agencies had information security issues reported. These audits have raised a significant awareness across agencies and we expect that necessary improvements are made.

In this audit we set out to assess whether agencies are adopting better practice in managing their information systems security. As our benchmark we used the International Standard (A/NZS ISO 27002:2006) for information security. Although these standards are not mandatory in Western Australia they are a good starting point for an agency to develop sound information security practices. The implementation of most categories of the standards would see our findings in security diminish considerably.

This security gap analysis provides further insight into how big the gap is between the standards and a representative sample of the WA public sector.

What was done

The security gap analysis was conducted across 21 agencies as part of our annual general computer controls audits. We assessed information security across all security categories defined within the international standard. There are essentially 12 areas the standards focus on with each area containing various categories. The areas are:

- Physical and Environmental Security
- Security Policy
- Access Control
- Human Resources Security
- Organising Information Security
- Communications and Operations Management
- IS Acquisition, Development and Maintenance
- Compliance
- Asset Management
- Information Security Risk Management
- Information Security Incident Management
- Business Continuity Management

We assessed whether controls for the categories in each area were effectively being met and if not whether mitigating controls were in place. As part of the assessment against the standards we also assessed the following:

- Have agencies identified their security requirements by assessing the risks to their business and information systems?
- Have agencies selected appropriate controls that mitigate their identified risks, in line with the International Standard?
- Where agencies are not aligned with the International Standard, have other strategies been used to mitigate identified risks?
- What is the degree of alignment with the International Standard across all information systems security categories?

Each area was assessed in terms of its effectiveness in meeting the standards and scored. We rated scores above 85 per cent to be effective, scores between 60 to 85 per cent as partially effective and below 60 per cent as ineffective. Those areas in the standard that were obviously not applicable to the agencies we audited were not considered.

What was found

Table 1 below represents the results of our gap analysis across the 21 agencies. None of the 21 agencies fully met the requirements of the standards however two agencies came close. Ninety per cent of the sampled agencies had serious shortfalls in meeting the security standards across multiple categories. It is likely that this result is relevant to most agencies across government and demonstrates a lack of good security practices across the Public Sector. This in turn puts agency systems at risk. We noted that the size of an agency had no bearing on good or bad security practices.

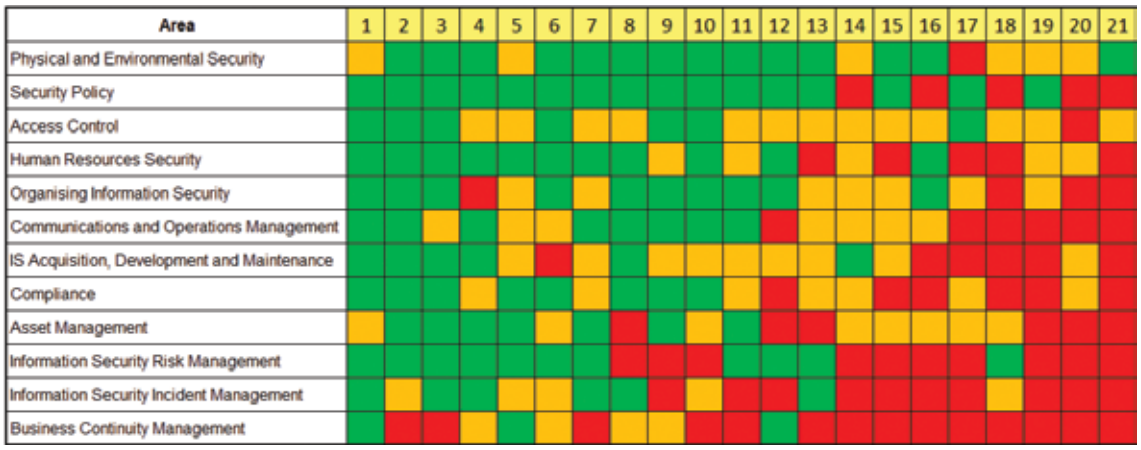


Table 1: Results of security gap analysis for 21 agencies

Red = ineffective, Orange = partially effective, Green = effective

Analysis of results

The standards provide guidance on how an organisation should approach information security. The starting point is establishing what the security requirements are and assessing risk. Security requirements can be derived from three main sources which include (1) assessing risks taking into account the overall business strategy and objectives. (2) The legal, statutory and regulatory requirements including contractors, service providers and partners. (3) The principles, objectives and business requirements for information processing to support operations.

Our analysis indicated that many of the agencies are not taking these first steps by adopting a strategic approach to identifying and assessing risks. This can be seen in Table 1 which shows that only half of the agencies rated well in the Information Security Risk Management category. This is an important area of initial focus to identify, assess and treat risks and allows agencies to take a strategic approach to managing information security. In the absence of a strategic approach agencies lack focus and the approach to security becomes ad hoc. This can lead to agencies wasting resources on areas of minimal risk while leaving critical areas exposed.

Agencies should use their risk assessment to inform the development of business continuity and specific incident management plans. A sound information security policy is important for security governance and should also be informed by the initial risk assessment. Table 1 illustrates that agencies that met the standards in these areas generally did better across all other areas. However a common failing was lack of business continuity management for information security. These plans help to ensure agencies can recover or continue to function should a serious incident occur.

Where agencies had not performed a risk assessment they typically demonstrated weaknesses across all areas. Table 1 shows that eight agencies had inadequate controls for at least nine of the 12 areas assessed. This demonstrates a lack of awareness and understanding of the controls required to ensure the security of their environments.

Fifteen agencies did not have effective controls in place for Information Security Incident Management or IS Acquisition, Development and Maintenance. These agencies will not be able to detect and respond to incidents that threaten the security and availability of their environments. Key applications within these agencies are also more vulnerable to unauthorised access and downtime.

Our analysis suggests agencies are focusing on some quick wins such as physical and environmental security, but may be missing some of the more significant areas as highlighted above.

Security Standards – addressing the gaps

Agencies can use the standards to perform their own gap analysis and use the results to develop a security improvement plan. This can provide a foundation for setting priorities, assigning ownership, allocating investments of time, money and human resources and for measuring and improving compliance with the standards.

Information security is achieved by implementing suitable controls including policies, procedures, organisational structures and software and hardware functions. These controls need to be implemented, monitored, reviewed and improved where necessary to ensure that specific security and business needs of an agency are consistently met.

Depending on each agency's business objectives and circumstance, all areas of the standard could be equally important. Agencies need to take a methodical approach when performing a risk assessment to identify and understand the level of control required for each area. Costs for implementing controls must be balanced against the likely impacts resulting from identified security failures. Risks assessments also need to be re-performed periodically to ensure new risks are captured and managed in a timely manner.

While the International Security Standard is a good starting point, additional controls and guidance may be required depending on agencies' specific needs and functions. The Defence Signals Directorate (DSD) produces the Australian Government Information Security Manual (ISM). The manual is the standard which governs the security of government ICT systems. It complements their Protective Security Policy Framework and is a good reference for understanding and implementing good information security practices.

Application Controls Audits

Background

Applications are the software programs that are used to facilitate key business processes of an organisation. For example finance, human resource, licensing and billing are typical processes that are dependent on software applications. Application controls are designed to ensure the complete and accurate processing of data from input to output.

Each year we review a selection of key applications relied on by agencies to deliver services to the general public. Failings or weaknesses in these applications have the potential to directly impact other organisations and members of the general public. Impacts range from delays in service to possible fraudulent activity and financial loss. This report describes the results of key application reviews conducted at four agencies.

What did we do?

We reviewed five key business applications at four agencies. Each application was selected on the basis of the significant impact on the agency or the public if the application was not managed appropriately.

Our application reviews involve an in-depth focus on the step by step processing and handling of data. Our main purpose for reviewing computer applications is to gain assurance that:

- **Policies and Procedures** – appropriate policies and procedures are in place to support reliable processing of information
- **Data Preparation** – controls over the preparation, collection and processing of source documents are accurate, complete and timely before the data reaches the application
  - **Data Input** – data entered into the application is accurate, complete and authorised
  - **Data Processing** – is processed as intended in an acceptable time period
  - **Data Output** – output including online or hardcopy reports, are accurate and complete
- **Interface Controls** – controls are suitable to enforce completeness, accuracy, validity and timeliness of data transferred
- **Master File Maintenance** – controls over master file integrity are effective which ensure changes are approved, accurate and complete
- **Audit Trail** – controls over transaction logs are in place which ensure transaction history is accurate and complete

- **Segregations of Duties** – no staff performed incompatible duties
- **Backup and Recovery** – the system/application can be recovered in the event of a disaster.

This year we reviewed the following agencies and applications:

1. **Firearms Management System** – Western Australia Police
2. **ProgenNET** – Department of Finance
3. **Emergency Department Information System** – Department of Health
4. **Hospital Morbidity Data System** – Department of Health
5. **Royalties Online** – Department of Mines and Petroleum

Figure 1 represents the main elements: people, process, technology and data that are the focus of our application reviews. In consideration of these elements, we follow the data from input, processing, storage to outputs.

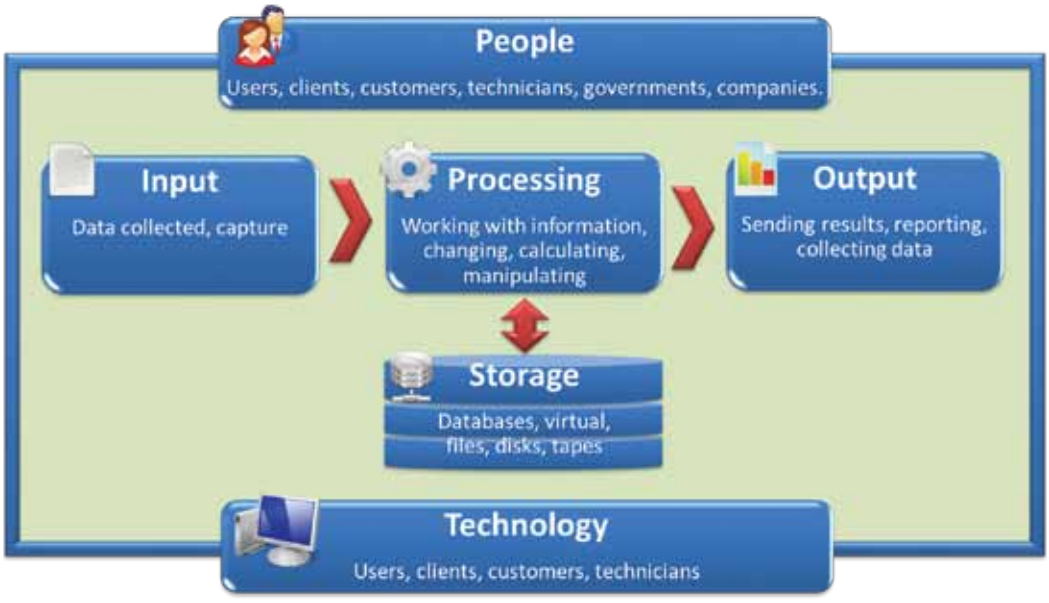


Figure 1: Areas of focus for application reviews

Firearms Management System – Western Australia Police (WAP)

Conclusion

The Firearms Register and supporting systems have numerous weaknesses in the controls over data input, processing and reporting. As a result we have no confidence in the accuracy of basic information on the number of people licensed to possess firearms or the number of licensed or unlicensed firearms in Western Australia. In the absence of reliable information, WAP are unable to effectively manage firearms licensing and regulation in WA.

Background

Firearms licensing in Western Australia is governed by the *Firearms Act 1973* and the Firearms Regulations 1974. Under the Act, a person wishing to possess or use a firearm must have a firearms licence. A licence may be issued to either an individual person or to a body corporate such as a security company.

To obtain a firearms licence, a paper based application form and supporting documentation is submitted to WAP electronically via Australia Post. The application includes the following information:

- Genuine reason – There must be a genuine reason to hold a firearm licence. This includes membership of a shooting club, recreational shooter or a collector. Licence holders may also have an occupational requirement such as a primary producer or security firm properly licensed under the *Security and Related Activities (Control) Act 1996*.
- Firearms awareness certificate – People who are applying for their firearms licence for the first time (original application) are required to complete a firearms awareness test. This is conducted at an approved firearm association or club and a 28-day cooling off period exists after submitting the application.
- Firearms serviceability certificate – All firearms subject to a licence application, or subsequent additions to a licence, must be accompanied with a serviceability certificate which is obtained by the seller.
- 100 point proof of ID

- Other supporting documentation such as:
  - where the licensee is a primary producer – proof of property ownership
  - where the licensee is not a primary producer – a 'property letter' from a primary producer allowing the licensee to use the firearm on their property for a legitimate purpose
  - where the firearm is to be used at a gun club – a club or association support letter
  - where the firearm is to be used for work – an occupational requirement disclosure, certificate of incorporation and registered business name.

Once approval of the application has been given by WAP, the applicant must provide photographic evidence of secure storage for the firearm. This must also be accompanied by a statutory declaration for the evidence provided. WAP will then proceed with the processing of the application prior to issuing a firearms license.

Diagram 1: Original Firearm Application Process overview

Police are responsible for:

- assessment of all applications for firearm licences and the addition of firearms to existing licences
- renewal and cancellation of firearms licences
- regulation of commercial organisations involved in the sale, manufacture and repair of firearms and ammunition
- retrieval of firearms as required

WAP is required by the *Firearms Act* to maintain a register of all licensed firearms. The register used is called the Firearms Registry System (FRS). The register includes a unique identifier for each firearm, information on who is licensed to use it, how it can be used, and where it must be stored.

We conducted performance audits on the management and regulation of firearms in 2000, 2004 and 2009. In each report we identified various problems with the systems and processes for the licensing and management of firearms in Western Australia. Our 2009 report raised specific concerns with the Firearms Register and related systems. The issues raised meant that WAP could not rely on the accuracy of the information held in the register.

Following the 2009 report the WA Parliament's Public Accounts Committee requested WAP provide an update of progress for fixing the issues we had identified with the Firearms Register. WAP reported to the Committee in September 2011 that a stabilisation project was commenced in early 2010 and concluded in May 2011. The project cost was reported as approximately $720 000. WAP advised the Committee that as a result of the project the Firearms Systems are 'stable, satisfactory and functional'.

We reviewed the Firearms Register and supporting systems to determine whether they were operating effectively

Key findings

We identified some concerning issues that result directly or indirectly from the lack of reliable data and difficulties in accessing basic management information from the Firearms Registry System. These issues include:

- **Firearms not recovered from deceased estates** – 988 firearms have not been recovered by WAP from deceased estates dating back to 1983. No records could be found in the Incident Management System (IMS) or Firearms Registry System (FRS) to ascertain if the firearms had been seized.

  After a person passes away it can take up to 280 days before FRS is updated with this information so that WAP can commence with recovering the firearms. FRS is only updated when a renewal notice is issued not when they are deceased. During this time the firearms belonging to the deceased licence holder remain unaccounted for.

- **Use of template 'property' letters** – a recreational firearm licence must have an accompanying (property) letter of approval from a property owner to use the licensed firearm on their property. There is no limit to the number of property letters that can be issued by an individual property owner. However, FRS does not have the capability to search or report on the number of property letters associated with each property.

  During the course of our audit we became aware of at least one case where a person was sold a property letter by a firearms dealer so that they could apply for a firearms licence. As a consequence we sampled a small number of firearms applications and found that one property owner had provided property letters to over 270 applicants

over the past 17 months. We noted that these firearms had all been purchased from the same firearms dealers. Similarly we found another case where over 80 property letters had been provided by the same property owner for firearms purchased from a single dealer.

WAP advised this practice is not illegal but acknowledge it is not in accordance with the intention of the legislation and expect this issue will be addressed through a proposed review of the Act. They further advised that the properties in question are a significant size, being 7 614 and 3 000 square kilometres respectively. As a safety measure one of the property owners maintains a register of when people shoot on their property.

We note that a licence holder is not limited to using their firearm on the property listed on their original application once their licence is approved.

- **People assessed as unfit to have a firearm still listed as possessing them** – over 300 firearm licence holders still had firearms listed against their licence despite being classified by WAP as unfit to possess a firearm. Reasons why people are classed as unfit to possess firearms include having a criminal conviction or being the subject of a violence restraining order.

  We advised WAP of this issue during the course of the audit. They advised they were aware of it prior to our audit and had commenced a review to determine the accuracy of the information. At completion of our audit, they had followed up approximately 50 per cent of the 'unfit to issue' licence holders listed in the system and found no firearms in the possession of these licence holders.

  WAP found in some cases a firearm had been seized but this had not been recorded in the system. In other cases the firearm was in the possession of a co-licence holder however again this was not recorded in the system.

- **Limited capacity for management reporting** – FRS does not have the capability to produce simple management reports. For example in order to produce a simple report on the number of expired licenses a request for service needs to be submitted to another branch of WAP for it to be produced. We requested verification of previously reported firearms statistics. WAP informed us that this report would take more than five working days to process and indicated that they could not guarantee the accuracy of the information requested. As a result of these issues, staff manually create management reports in spread sheets.

- **Errors in updating information on the national CRIMTRAC database** – we found over 25 000 instances where data could not be reconciled between the WAP firearms register and the national CRIMTRAC database. Of these, over 1 000 are linked to deceased estates and persons unfit to issue. The remaining 24 000 relate to the

reason and conditions associated with the issue of a firearms licence. These errors are caused by data incompatibilities between the systems. This means the national database may not contain up-to-date or accurate records for WA firearms or licensees.

- **Nominated persons register** – details of nominated persons who have access to firearms under a corporate license but do not require an individual firearms license are maintained in a spread sheet completely separate to the firearms register. There is a risk to the integrity of the information due to the possibility of unauthorised access, and there are no audit trails or history of changes. Data could also be lost due to human error.

Other issues we noted included:

- **Firearm identification card** – we identified a number of concerns with Firearm Identification Cards including persons having more than one card, signatures missing from applications, photo of person did not match the license holder's name, and cards with no details. Incorrect information on the cards creates a range of identity and security risks.
- **Workarounds and manual processing** – manual processing is required for FRS to effectively operate. This includes the need to reconcile the accuracy of data back to IMS and other WAP systems and then manually change information as required. This process creates an increased risk of errors.
- **Access and logging** – we found no policies or procedures in place relating to log access, changes and reviews of logs for databases. WAP use an application called Auditrak for logging user activities and changes. We found Auditrak's usefulness to be limited because it only logs user activity made at the user interfaces of the relevant applications and not in the database or test environments that store this information. This means that unauthorised access will not be detected.

  We also found that some of WAP's Business Technology (BT) managers had 'senior administrator' access rights that were not required for their roles. These rights meant that the BT staff were able to read, delete or alter the firearm history of license holders undetected. The confidentiality of the data is also at risk.
- **Australia Post contract** – when requested WAP were unable to provide the contract with Australia Post for firearms application processing, fee collection and letter printing. Without effective contract management, WAP may not be aware of costs and Australia Post's obligations to meet agreed performance. Applications may be lost or not processed in the specified time.

Recommendations

Western Australia Police must:

- ensure that the integrity and timely input of information into firearms management systems is performed to ensure that firearms can be suitably managed
- ensure that business requirements for the new firearms management systems are adequately defined to ensure they support the business of managing firearms. Strong consideration needs to be given to management reporting. Good project management practices are essential from initiation to completion
- retrieve firearms from deceased estates promptly and ensure that the information is entered correctly into firearms management systems
- ensure effective verification of information and supporting documentation provided by firearms license applicants
- review controls for logging and monitoring of access and changes to back end systems including the Databases and Servers that support firearms management
- consider developing recommendations for amendments to the *Firearms Act 1973* and the *Firearms Regulations 1974.*

Agency response

The Western Australia Police acknowledge the issues in the current Firearms Registry system, all of which Police have been aware of and responding to whilst developing the new Licensing and Registry system. Full implementation of the new system should address these issues, however is dependent on funds being made available. The Western Australia Police will continue its endeavour to improve its capacity and competence to fulfil its obligations under the *Firearms Act 1973*.

ProgenNET – Department of Finance

Conclusion

Overall ProgenNET is working properly with no significant control weaknesses identified. As a result we have confidence in the accuracy of information used to calculate lease charges and for the ongoing management of leases, tenants, landlords and other aspects of government office accommodation.

Background

Building Management and Works (BMW) within the Department of Finance, is responsible for coordinating the effective delivery and ongoing operation of the State Government's office accommodation needs. In August 2012 the Department of Finance reported that its centrally managed portfolio included 404 buildings covering 547 200m^2. This accommodation was leased to government agencies through 537 separate leases with a net annual rental cost of $181.2 million.

To effectively manage its portfolio of leased accommodation BMW uses a property management system known as ProgenNET. This system is used to calculate lease costs or charges and for the ongoing management of leases, tenants, landlords and other aspects of government office accommodation.

Lease documents provide the key input data for the system. Core information relating to elements of a lease entered into the system includes:

- location
- tenant
- landlord and service providers
- dates of commencement, review and renewal
- basis for invoicing or making payments as required under a lease (e.g. lease area and outgoings)
- costs or charges of the lease which links the above information and reflects the Lease Agreement.

Based on data from the lease documents entered into ProgenNET, invoices are issued to tenants and payments followed up by the Finance section of BMW. We conducted an initial review of the system as part of a performance audit reported in 2013. We identified a number of issues with the system at that time and the Department advised they were addressing them.

Key findings

Although we found that ProgenNET is working properly, we also found a number of issues that should be addressed. These include:

- The service agreement with the application support provider does not specify the level of service required or document a mechanism for adjustments to the annual maintenance service fee paid by BMW. The services provided by the support service provider for ProgenNET include:
  - telephone response to IT queries (helpdesk)
  - software consulting
  - customer staff training
  - site reviews
  - ongoing advice and assistance.

  The annual maintenance service fee for these services was initially set at $24 000, and gradually increased to $48 840 in 2012. However we noted that the level of service had not increased in line with the increased charges and there was no evidence that adjustments to the annual maintenance service fee were based on a review or evaluation of the services delivered. We found the only services provided by the service provider were responding to 63 support calls made over a 3 year period, 2010-12. These calls were classed as Normal (47), High (12) or Critical (4).

  With no Service Level Agreement in place, there is a risk that BMW service level expectations will not be met, which could impact on the availability and performance of ProgenNET. BMW may be paying excessive fees for the level of service they are receiving.
- A number of minor control issues were identified in relation to user access, password settings and monitoring of logs. For example:
  - **User access** – nine out of 32 ProgenNET users had administrator level access which was not required based on their roles. This has since been reduced. Users with administrator level access can create, remove and modify user accounts, lease data and log files.
  - **Passwords** – passwords in ProgenNET were set to expire in 185 days instead of 90 days as specified in their policy
  - **Monitoring** – logs generated by ProgenNET are not monitored and regularly checked for any suspicious or irregular activities.

Recommendations

The Department of Finance (BMW) should:

- setup a formal service level agreement with its service provider that clearly defines service levels and performance measures and maintenance fees
- setup a process to regularly review logs and follow up on exceptions and ensure that password controls are in-line with its password policy
- review user accounts to ensure that privileges and user access is appropriate at all times including accounts affected by termination or change of employment.

Agency response

The Department of Finance accepts all the recommendations made by the Office of the Auditor General. Substantial progress has been made in implementing the recommendations and it is anticipated that all the required improvements will be in place by December 2013.

Emergency Department Information System (EDIS) – Department of Health

Conclusion

EDIS was found to be an effective application for managing workflows in the emergency department. However some control weaknesses were identified during the audit. These control weaknesses mean that staff could anonymously alter data relating to treatments provided and times of admission and discharge. We analysed data logs captured by the system over the last two years against data entered by staff and found no alterations had occurred.

Background

The Department of Health (Health) is responsible for providing emergency department services to the people of Western Australia. In the 12 months to 30 June 2012 a total of 975 286 people attended emergency departments state-wide.

Health uses the Emergency Department Information System (EDIS) to assist in the management of emergency departments. This system is both a workflow and a data collection tool designed to capture real-time information about patients, and to support the operational control of Health (i.e. Metropolitan Hospitals plus Bunbury) emergency departments. EDIS is used when a patient presents to an emergency department to capture key information including:

- patient identity (unique identifier generated or existing in the system) such as date of birth, address, occupation, next of kin
- insurance status (Medicare or Private)
- admission time
- mode of arrival (e.g. ambulance, private transport)
- treating medical professional (e.g. doctor or nurse)
- primary diagnosis
- outcome (i.e. admitted to hospital or discharged)
- discharge and departure date

Data from EDIS is used for emergency department (ED) performance and management reporting. This includes:

- achievement of Activity Service Targets for ED attendances
- percentage of ED patients admitted, transferred or discharged within four hours
- percentage of unplanned re-attendances within 48 hours

We tested performance information reported by reconciling it back to production databases and assessed the controls that preserve the integrity of this process. Each instance of EDIS can be configured and implemented differently in each Hospital. We reviewed EDIS at three metropolitan hospitals.

EDIS links to other Health systems such as PAS, TOPAS and MediTech which are patient administration systems. These systems record each patient's demographics (e.g. name, home address, date of birth) and all patient contacts with the hospital, both outpatient and inpatient.

Key findings

We found that limited system controls exist to detect and prevent users from gaining unauthorised access to confidential information. The EDIS application has been configured with limited logging of user activity. This means that individual staff activity cannot be identified.

Without adequate controls to prevent or detect direct access to the EDIS database there is a risk to the security of patient records maintained by Health. This could result in unauthorised disclosure of patient information and reputational damage to Health. In the absence of appropriate and reliable activity logs any unauthorised access cannot be conclusively linked to staff.

Health has identified a number of issues relating to the last upgrade of EDIS which is affecting clinical work practices. These issues impact on the Emergency Departments ability to process information efficiently and on the integrity of information relied on by Health. Examples include; ambulance ramping information cannot be determined accurately and initial triage assessments can be overwritten with no traceability.

We also found that EDIS does not require validation of the identity of each person making clinical data entries. Therefore, Health cannot determine which medical staff are responsible for clinical data entries made in EDIS or for data entry mistakes that result in adverse patient care.

Recommendations

Health should:

- improve change management controls so that unauthorised or inappropriate changes are prevented or tracked after the initial entry of data into EDIS.
- consider implementing user authentication for each staff member and logging their activities and changes made in EDIS. Health should also monitor high risk activities and changes made.
- ensure EDIS is configured to force users to comply with its password policy
- consider preventative and detective controls to help limit unauthorised access and data leakage
- maintain a risk register to ensure the risks associated with EDIS are identified, have a risk owner, an appropriate whole of health risk treatment plan, and a risk review schedule.

Agency response

The Department of Health, on behalf of the state public health sector, accepts the findings and, noting that appropriate action has already been taken to address many of the issues, supports the recommendations made by the Auditor General

Hospital Morbidity Data System – Department of Health

Conclusion

The Hospital Morbidity Data System (HMDS) was found to be operating as designed. However we found a few control weaknesses. The main weaknesses relate to the risk of unauthorised access to morbidity data. This can occur through insecure methods used to obtain and transfer data or because recommended software security updates are not implemented. While the system is working effectively, the identified weaknesses pose an unacceptable risk to the integrity and confidentiality of morbidity data and patient information.

Background

The Hospital Morbidity Data System (HMDS) contains a record of personal and medical information of all patients admitted to public and private hospitals including Emergency Departments in Western Australia. Under the *Hospital and Health Services Act 1927*, the Department of Health (Health) requires all public and private hospitals to submit activity data to the HMDS in accordance with agreed data management protocols. For each record there are more than 200 data elements captured. Each data element can be divided into two sections:

- Non-Clinical Data (e.g. patient demographics, admission and discharge details)
- Clinical Data (e.g. diagnoses, procedures, external cause and details of the condition)

The HMDS provides Health with the necessary information for planning, allocating and evaluating health services within Western Australia. This information is also used to meet mandatory and statutory reporting requirements and to support funding arrangements with the Commonwealth Government. The system contains over 20 million electronic inpatient records dating back to 1970, with approximately 850 000 records added in 2011-12.

Key findings

Specifically we found that Health is using insecure methods to obtain patient information from private and public hospitals. Patient information was collected from private hospitals using thumb drives and from public hospitals using an insecure file transfer protocol (FTP) which sent information in clear text across the network. Both of these methods leave the information vulnerable to unauthorised access.

It was noted that Health does not have an effective process in place to ensure that software updates are applied to critical servers as recommended by vendors. These updates are essential to maintain the security of systems.

We noted evidence of data mismatching between HDMS and data recorded in public hospital systems (TOPAS and HCARE). The results of testing carried out for 2011-12 show 1 328 instances of data mismatches between HDMS and HCARE and 2 982 mismatches with TOPAS. It was identified that these mismatches occur as changes to existing records within TOPAS/HCARE are not re-sent to HDMS due to access privileges limitations within systems for HCN staff. However, given the small amount of mismatched data compared to the volume of patient data processed each year, there is minimal risk to the overall integrity of information being reported.

We found a number of generic accounts with privileged access to HDMS which are used for day to day tasks by Health staff and external contractors. In addition, these accounts were not linked to staff identification numbers. Without effective controls over highly privileged accounts, there is an increased risk of unauthorised or unintentional modification or misuse of the system and key data.

Recommendations

Health should:

- assess the risk of using insecure methods for transferring public and private hospital morbidity information to HDMS. For private hospitals, Health should consider enforcing secure mechanisms for transporting data, where appropriate. For instance, using encryption or secure web access. For public hospitals, Health should also assess the risk of using an insecure mechanism (FTP) for transferring morbidity data to HDMS.
- ensure all changes to source morbidity data recorded in TOPAS and HCARE are appropriately synchronised to HDMS to avoid the risk of data inconsistency
- review the current procedures for applying software updates to its systems to ensure all vendor security updates are assessed, tested and if applicable applied within a timely manner across all systems
- ensure privileged accounts to HDMS are reviewed periodically to ensure the level of access privileges is appropriate at all times.

Agency response

The Department of Health, on behalf of the state public health sector, accepts the findings and, noting that appropriate action has already been taken to address many of the issues, supports the recommendations made by the Auditor General.

Royalties Online – Department of Mines and Petroleum

Conclusion

The Royalties Management System was found to be operating effectively. Only minor issues were identified during the audit and all where promptly dealt with by the Department and no longer pose any long term risk.

Background

Mining Royalties represent a significant source of revenue for the State Government. Royalties collected from mineral and petroleum producers in Western Australia for the 2011-12 financial year amount to approximately $4.9 billion.

Royalties are payments made by the mineral and petroleum producers to the State Government as compensation for the depletion of non-renewable resources. Royalties are payable monthly or quarterly and are the result of a self-assessment process undertaken by the producers.

To assist in monitoring and administering royalties the Department of Mines and Petroleum uses the Royalties Management System (Royalties Online). The key input document is the Royalty Return, similar to a tax return that is submitted by a mineral and/or petroleum producer. The return must be in an approved form, showing where relevant:

- quantity of the product mined or produced
- details of any sale, transfer, shipment or disposal of the mineral
- royalty value of the mineral
- gross invoice value of the mineral, when it was paid, and any allowable deductions for the mineral
- rate of royalty used

Royalty Returns are subject to audit by the Department at least once every three years. The royalty returns can be prepared and lodged online via Royalties Online. Payments are made either by electronic funds transfer or cheque. Once payment is received a Journal transfer to the financial system is automatically generated by the Royalties Management System. The system also provides for the Department to monitor and follow up issues such as overdue payments and overdue returns.

Key findings

Audit found that the system is relatively new and that ongoing testing and evaluation is being performed by the Department to ensure that data integrity issues are identified and resolved as they arise. To date the Department has been able to promptly rectify any identified issues.

Recommendations

The Department should continue with its work to complete testing of the Royalties system. All system aspects should be tested methodically to ensure management's expectations are met and the integrity of the system is upheld.

General Computer Controls and Capability Assessments

Conclusion

We reported 375 general computer controls issues to the 44 agencies audited in 2012.

From the 36 agencies that had capability assessments conducted only three were meeting our expectations for managing their environments effectively. Half of the agencies were not meeting our benchmark expectations in three or more categories.

Management of Changes and Physical Security were being managed effectively by most agencies, the Management of IT Risks, IT Security, Business continuity and Operations need much greater focus.

Background

The objective of our general computer controls (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 2012 we focused on the following control categories:

- IT operations
- Management of IT risks
- Information security
- Business continuity
- Change control
- Physical security

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 at 44 agencies and did capability assessments at 36. This is the fifth year we have been assessing agencies against globally recognised good practice.

We provided the 36 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 that of ours which was based on the results of our GCC audits. The agreed results are reported below.

We use a 0-5 scale rating[1] listed below 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 these agencies from year to year. Our intention is to increase the number of agencies assessed each year.

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)

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

What did we find?

Our capability maturity model assessments show that agencies need to establish better controls to manage their IT operations, IT risks, information security and business continuity. Figure 2 below summarises the results of the capability assessments across all categories for the 36 agencies we audited. We expect agencies should be at least within the level three band across all the categories.

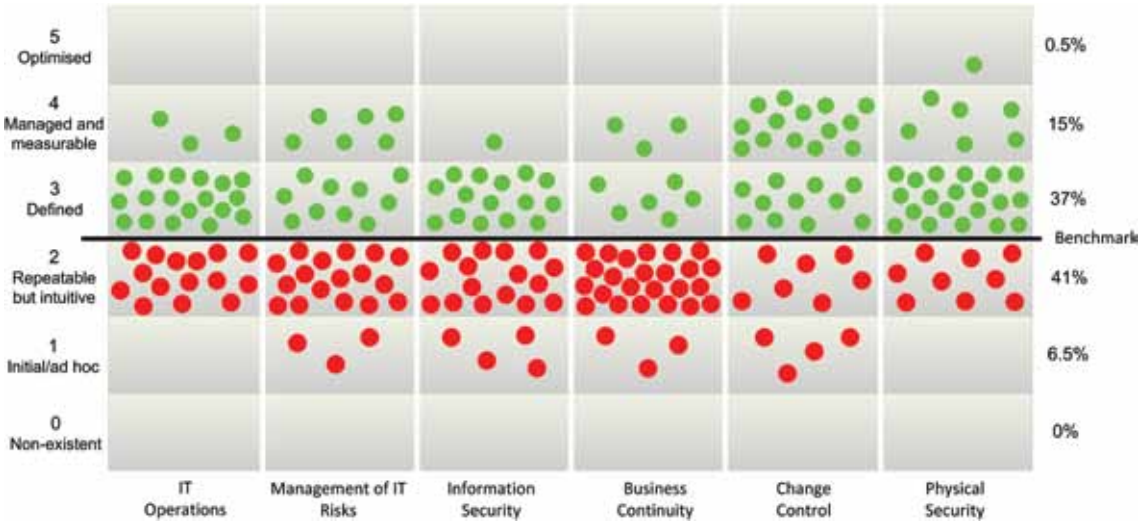


Figure 2: Capability Maturity Model Assessment Results

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 three or above for individual categories was as follows:

- IT operations 58 per cent
- Management of IT risks 44 per cent
- Information security 44 per cent
- Business continuity 25 per cent
- Change control 69 per cent
- Physical security 75 per cent

Three of the 36 agencies were assessed as level three or above across all categories. Half of the agencies did not achieve level three rating for three or more categories.

Eight agencies made improvements in at least one of the categories without regressing in any category. Nine agencies showed no change. Seven agencies moved up in one category but went down in another. Four agencies regressed in at least one area without making any improvements.

Eight agencies were assessed for the first time this year. The agencies that we assessed for the first time are generally not better or worse than those that have had ongoing assessments. The results of our work show that some agencies have implemented better controls in their computing environments however, most still need to do more to meet good practice.

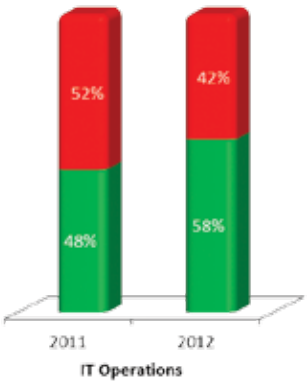
IT operations

This is the second year we have assessed IT operations for agencies. There has been an improvement with a 10 per cent increase in the performance of agencies improving on the service levels provided by IT to meet the agencies business requirements.

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. Some of the tests include 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.



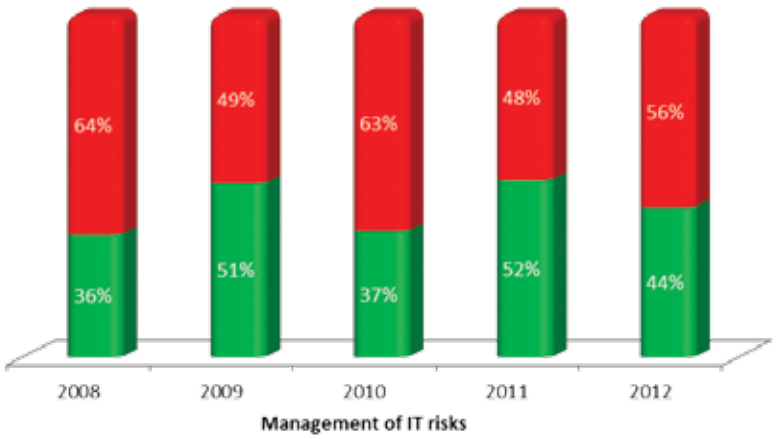
Examples of findings:

- a number of agencies have either no, incomplete or out-dated Information Security Policies
- one agency's process for managing the segregation of duties for users of its financial system was found to be ineffective. A sample found employees carrying out incompatible duties. In another agency system controls have not been implemented to prevent employees from performing the following processes:
  - raise purchase orders
  - authorise purchase orders
  - insert purchase orders' details in the system
  - receipt goods in the system
- at one agency there is no formal service level agreement in place that identifies the agreed service levels provided by their data centre service provider.

The following section highlights trends over the last five years for the remaining five GCC categories.

Management of IT risks

Fifty-six per cent of agencies did not meet our expectations for managing IT risks. This increased by eight per cent from 2011 when we found 48 per cent with issues in this area.



Examples of findings:

- a number of agencies did not have a risk management process for identifying, assessing and treating IT and related risks. Also many agencies still do not have a risk register for ongoing monitoring and mitigation of identified risks

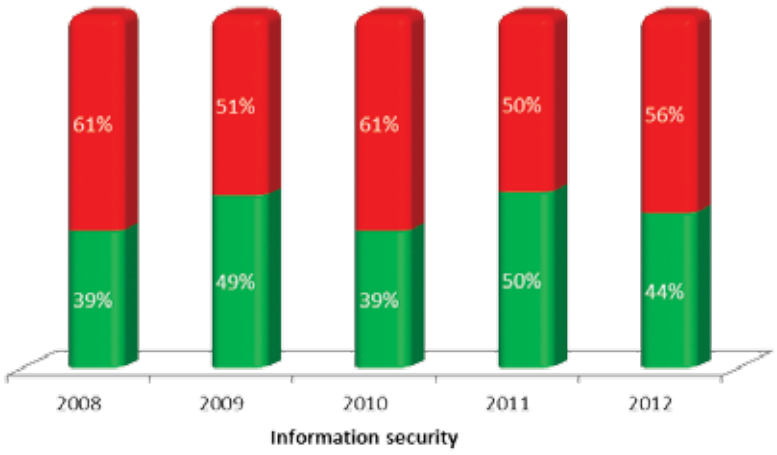
- the method currently used by one agency to assess their IT risks was inadequate or ineffective
- one Department's IT risks identified within their risk register have not been reviewed for the last 12 months to ensure the relevance of the risks and associated plans.

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

There was a six per cent increase in security issues from last year after an 11 per cent decrease in 2011. This means that 56 per cent of agencies are below our benchmark for effectively managing information security. It is clear from the basic security weaknesses we identified that many agencies have not implemented fundamental security controls to secure their systems and information.



Examples of findings:

- one agency did not have an effective process in place to ensure that critical software patches and security updates are identified and applied to the network environment and computer systems in a timely manner. Our scans identified a large number of critical and high priority patches which were not applied to databases, operating systems and servers. We also noted that the patching regime was done on an ad hoc basis

- at a number of agencies we found ineffective procedures regarding the monitoring and review of security logs and audit trails within key servers such as the network's Domain Controller and remote access server. Agencies were not pro-active in monitoring of logs to identify unauthorised actions or suspicious activities across the network servers
- we reviewed one department's user access lists for the network's Active Directory and Alesco system and found the following issues:
  - 11 active network users belonging to former employees, six of them had logged in to the network after their termination date.
  - six Alesco user accounts belonging to persons that neither exist on staff lists nor have corresponding network user accounts
  - 3 702 active network user accounts that have not been used to login to the network for over six months.

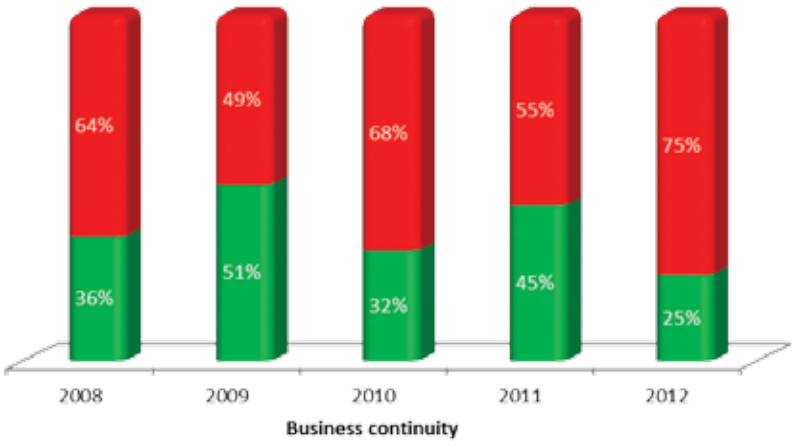
Information security is critical to maintaining data integrity and reliability of key financial and operational systems from accidental or deliberate threats and vulnerabilities. We examined what controls were established and whether they were administered and configured to appropriately restrict access to programs, data, and other information resources.

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 20 per cent increase in issues from last year. This is disappointing given the 13 per cent improvement in 2011. In 2012 more than 75 per cent of the agencies did not have adequate business continuity arrangements and 42 of agencies had these issues outstanding from the previous year.



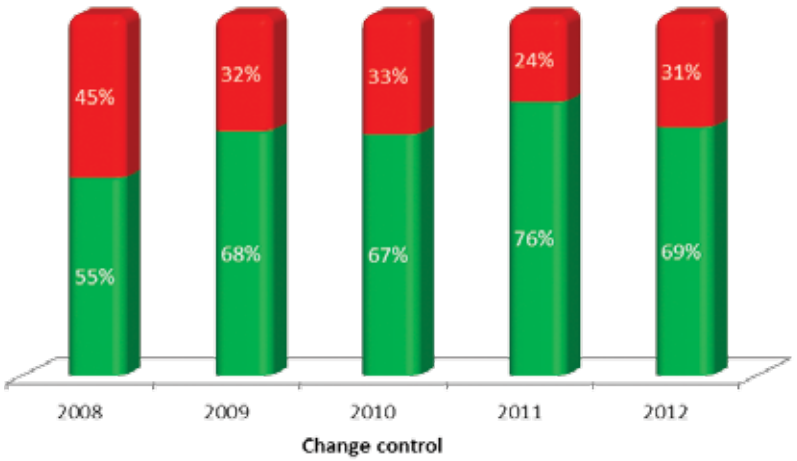
Examples of findings

- a number of agencies were found not to have a BCP or if they did have one it was either in draft or had not been reviewed for a number of years
- one agency did have a BCP but it was developed by a contractor and was no longer relevant to the existing environment. Also a number of business systems with their own BCP had plans that where out-dated and no longer usable.
- many agency DRP's had never been tested or approved and in one case the DRP did not reflect their environment and referred to some infrastructure, key personnel and contacts that were no longer applicable

Change control

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

There was a seven per cent increase in issues from 2011 in change control practices by agencies. This was after a nine per cent improvement from the previous year. However sixty nine per cent of agencies were still meeting our benchmark for change controls. We found issues at 31 per cent of agencies we reviewed which is a seven per cent increase on the previous year.



Examples of findings:

- we found that for many agencies there are no formal change management policies in place to ensure all changes to IT systems and applications are handled in a standardised manner
- at one agency the current change control procedure does not document important aspects of change management such as:
  - need to document, categorise, and test all changes before implementation into the operating environment. A sample of five change requests had no evidence of being documented before the changes were implemented into the operating environment
  - the processes for classifying and handling non-scheduled (emergency) changes

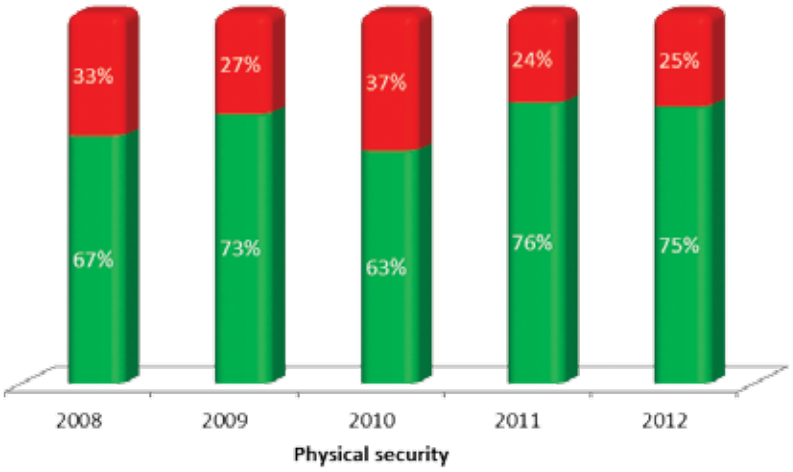
An overarching change control framework is essential to ensure a uniform standard change control process is followed, achieve better performance, reduced time and staff impacts and increase the reliability of changes. When examining change control, we expect defined procedures are used consistently for 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.

We found a one per cent increase in the number of issues from last year in agency management of physical security. Seventy five per cent of agencies where still meeting our benchmark.



Examples of findings:

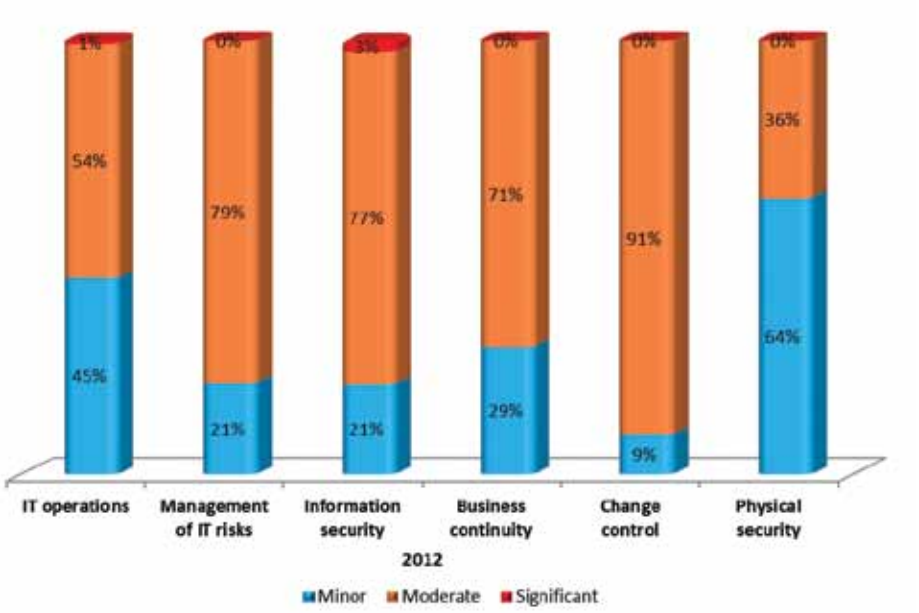
- at a number of agencies issues with the physical environment were noted:
  - installation and testing of the Uninterrupted Power Supply (UPS) was yet to be completed.
  - power generators to be used in the event of power failure had not been tested.
  - no fire suppression system installed within the server room
- a number of agencies were found not to have temperature or humidity monitoring configured to alert in the case of an event related to the server rooms
- some agencies continue to not appropriately restrict access to their computer rooms with staff, contractors and maintenance people having unauthorised access to server rooms. For example, approximately 40 people across one organisation have access to the computer rooms while the log detailing access to the computer room is not reviewed on a regular basis

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

The diagram below 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 serious exposure to risk.

The below diagram represents the 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 NUMBER	2013 REPORTS	DATE TABLED
10	Supply and Sale of Western Australia's Native Forest Products	26 June 2013
9	Administration of the Patient Assisted Travel Scheme	26 June 2013
8	Follow-up Performance Audit of Behind the Evidence: Forensic Services	19 June 2013
7	Fraud Prevention and Detection in the Public Sector	19 June 2013
6	Records Management in the Public Sector	19 June 2013
5	Delivering Western Australia's Ambulance Services	12 June 2013
4	Audit Results Report - Annual Assurance Audits: Universities and state training providers and Other audits completed since 29 October 2012 – and Across Government Benchmarking Audits: Recording, custody and disposal of portable and attractive assets and Control of funds held for specific purposes	15 May 2013
3	Management of Injured Workers in the Public Sector	8 May 2013
2	Follow-on Performance Audit to 'Room to Move: Improving the Cost Efficiency of Government Office Space'	17 April 2013
1	Management of the Rail Freight Network Lease: Twelve Years Down the Track	3 January 2013

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