Information Systems Audit Report

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
8 April 2009

Contents

Auditor General's Overview

Information Systems (IS) audits are a key component of my office's work. Previously the results of the IS audits have been incorporated into our financial and performance audit reports. But this year for the first time we are reporting the results of our IS audits in a stand-alone report. This reflects the importance of IS matters in government.

The report covers three items and is divided into two sections:

- IS Compliance Audit
    - Protection of personal and sensitive information
- General Computer and Application Controls Audits
    - General Computer Controls
    - Application Controls

The first item of the report raises some concerning issues and is a wake up call to all government agencies that handle personal and sensitive information. I found fundamental weaknesses in all of the key areas of information security at the agencies examined. I was sufficiently concerned by this that I have sought assurance from agencies that our recommendations were being implemented.

The results of the general computer and application controls audits reinforces my concern that many agencies are continuing to ignore the importance of effectively managing their information systems. For general computer controls, we reviewed 65 agencies and benchmarked 41 against accepted good practice for IS management. Nearly 60 per cent of agencies failed to meet the benchmark. Our audit of five key business applications found weaknesses in security and data processing controls that could potentially impact delivery of key services to the public.

By failing to address fundamental control weaknesses, agencies leave themselves vulnerable to computer system failures, unauthorised access to information, loss of information and fraudulent activity. Many of the controls required to ensure appropriate and secure management of an organisation's computer systems do not require expensive technology or large numbers of specialist resources. Good controls can be achieved through the appropriate implementation and management of basic polices, procedures and practice.

I expect agencies across government to take note of the findings and recommendations of this report.

IS Compliance Audit

PROTECTION OF PERSONAL AND SENSITIVE INFORMATION

Overview

Personal information is information that identifies an individual such as name, address, date of birth, phone numbers and e-mail address. Sensitive information includes private details about an individual such as tax file number, next of kin, criminal and legal records, education, health details and financial status.

Western Australian Government agencies collect and store large amounts of personal and sensitive information about individuals. Members of the public have the right to expect that information about them is protected from unauthorised access or inappropriate use. Agencies in turn have a responsibility to ensure appropriate levels of security are in place to protect and maintain the integrity of personal and sensitive information.

Generally the personal information which is collected on individuals ends up being stored and processed within databases. Databases facilitate the efficient storage, processing and sharing of large amounts of information. However, if databases lack adequate safeguards then unauthorised access, alteration and theft of large volumes of information can occur.

Weaknesses in the security controls of computer systems holding personal and sensitive information can expose agencies and members of the WA public to a variety of risks:

- inappropriate or accidental disclosure of personal and sensitive information which could affect an individual's safety or reputation or result in financial loss

- theft or modification of information for the purposes of criminal activity and financial gain including identity theft, fraud, bribery, email scams etc

- inaccurate and unreliable information held resulting in incorrect decisions and errors being made

- reputational damage to agencies and loss of public confidence.

There is a risk of unauthorised access to government databases via the Internet. However, research indicates that the greater risk to personal data, whether maliciously or accidentally, is from staff, contractors and service providers inside an organisation.

We selected five agencies across key sectors of government, who collect and store a wide range of personal and sensitive information. These agencies had various forms of financial, medical, legal and educational information for hundreds of thousands of people in WA. The objective of the examination was to establish whether the controls in place at the selected agencies were sufficient to protect personal and sensitive information. We do not publically report the names of agencies examined in our IS audits to minimise the risk they will be targeted to exploit reported weaknesses. Another reason is that our findings and recommendations are relevant across government and not just to the specific agencies examined.

Conclusion

We found that there was a lack of fundamental controls in place to protect personal and sensitive information. This meant there was a real and significant risk of inappropriate disclosure or access to the information held by those agencies. In numerous cases the agencies would have no way of knowing if data theft or manipulation had occurred.

Key Findings

Specifically we found:

- Three out of the five agencies lacked IT security policies. This indicates a lack of understanding of security requirements by senior management. This in turn means agencies were often operating without a full awareness of the threats and vulnerabilities posed to their IT environment. Nor did they have appropriate procedures or guidelines for staff on how to mitigate those risks.

- None of the agencies we examined was consistently applying simple administrative controls such as police checks or confidentiality agreements for staff dealing with personal or sensitive information.

- Computer network security was poor, weaknesses we found included:

  - active network accounts for former employees of agencies

  - generic accounts that allow individuals access to networks by unidentified individuals that had no passwords or easy to guess passwords. In one agency, by using these accounts and guessing passwords, Audit was able to access almost 700 000 sensitive records via the Internet

  - network account and password details for generic accounts 'posted' on computer monitors

  - three agencies that were not logging or monitoring network use or unsuccessful log on attempts

  - three agencies that were not updating network operating software in line with vendor recommendations to address known security vulnerabilities.

- There were fundamental weaknesses in the security controls for computer applications and databases. Specifically:

  - Two agencies were storing sensitive information using database applications that were grossly inadequate for that purpose. The applications had no password controls and a well known security weakness which allowed the initial log on screen to be bypassed providing full access to all information.

- Four of the agencies had active accounts belonging to former employees. These types of accounts provide opportunities for misuse by insiders with minimal chance of tracing the individual responsible.

- In two of the three agencies that used a specific database, system default database accounts remained active and set to their default password. Database vendors warn that security is most easily compromised by leaving default passwords unchanged for these accounts.

- In four of the five agencies examined we found a wide range of confidential documents and files saved to unsecured folders on network servers. In some of the agencies this meant that thousands of sensitive files and documents relating to members of the WA public could be viewed by anyone connected to the network.

- None of the agencies we examined had adequate controls to address the risk of portable USB devices such as thumb drives, that can be easily lost or stolen, being used to transfer or store personal and sensitive information. We found several instances where USB devices were directly connected to computers used to store sensitive information.

What Should Be Done

To help ensure the protection of personal and sensitive information, government agencies need to assess the threats and vulnerabilities to their IT systems and implement policies, procedures and practices to mitigate those risks.

Specifically agencies should:

- define and endorse an IT security policy that reflects the sensitivity of the information they store and the risks to that information. This should include identifying all instances of personal and sensitive information held and based on risk assessments ensure there is an appropriate level of security controls over the information. Relevant information security standards such as ISO27001 and ISO27002 as well as relevant vendor documents provide guidance on basic information security controls

- ensure all users who will be given, or who have access to personal and sensitive data have been appropriately screened by completing background and criminal record checks. In addition, ensure users understand and have signed appropriate confidentiality and acceptable use of information systems agreements

- ensure that network, applications and database security controls are in place, up-to-date, regularly tested and enforced.

Agency Responses

Three of the five agencies we examined chose to provide a response to the audit findings and recommendations. The three agencies responded as follows:

- The department agrees with the need to have strong controls to protect unauthorised access or inappropriate use of confidential information and has already taken the necessary steps to implement the Office of the Auditor General Recommendations to strengthen controls in this area and hence provide confidence that information is appropriately protected.

- The audit findings in respect to this agency were classified moderate or minor but the recommendations proposed by the Auditor General were extremely useful in improving controls, compliance and accountability. Most of the recommendations have already been implemented and the remaining few are in the process of implementation.

- The agency agrees with the findings outlined in the report and upholds the need for strong protection of information. We have commenced implementation of several initiatives to strengthen governance in this area. These strategies will address several of the Audit recommendations.

Background

Personal information is considered to be information that identifies an individual (name, address, date of birth, phone number, email address etc). Sensitive information includes private details about an individual (e.g. tax file number, next of kin, criminal and legal records, education, health details, financial status).

We expect that agencies who hold personal and sensitive details about the public have established appropriate levels of information security to prevent unauthorised access or disclosure and to maintain the integrity of the information. Poorly managed databases containing personal and sensitive information can create significant security risks for the database owners and members of the public. In today's world, personal and sensitive information has a significant commercial value to individuals both in Australia and abroad.

Changes in technology now make information theft far easier and it is often more profitable than conventional forms of crime with less risk for the perpetrator. Though there is a risk of unauthorised access to government systems and information from over the Internet, research indicates that a greater risk, whether malicious or accidental, is from staff inside an organisation (agency staff, contractors and service providers).

Western Australian (WA) government agencies, unlike the Commonwealth and some other states[1], have no privacy legislation to provide regulatory guidance in relation to the collection, retention and security of personal information. An Information Privacy Bill was introduced to Parliament in March 2007; however with the recent change in Government the Bill would need to be reintroduced to progress towards legislation. In the absence of specific legislation, agencies should still have sound security practices and can take some guidance from relevant International Standards for information security such as ISO27001 and ISO27002.

What Did We Do?

The objective of the examination was to establish whether the controls in place at a selection of government agencies were sufficient to protect personal and sensitive information.

We selected five agencies across key sectors of government, who collect and store a wide range of personal and sensitive information. These agencies had various forms of financial, medical, legal and educational information for hundreds of thousands of people in WA.

This review was undertaken in accordance with the Australian Standards on Assurance Engagements as issued by the Australian Auditing Standards Board with a view to providing reasonable assurance under those standards.

---

1   Commonwealth – Privacy Act 1988, NSW – the Privacy and Personal Information Protection Act 1998 and Victoria – the Information Privacy Act 2000.

Within the information security arena the principle of 'defence in depth' is considered the most effective way to protect the confidentiality, integrity and availability of information. This is based on layers of security with specific sets of controls at each layer. The design combines these layers and controls to assist in the overall protection of the information. A graphical concept of the principle of security layers is shown in Figure 1.

Figure 1: Information Security Layers

The examination approach was to first identify the personal and sensitive information stored within the agency. Then based on our assessment of the most significant risks and vulnerabilities, we tested the adequacy of the controls in the following key areas:

- IT security policy – existence of an overarching policy that guides and informs the management approach to IT security generally

- administrative controls – security checks, confidentiality and acceptable use agreements

- network security – access controls, account management, logging and monitoring of users

- application and database security – access controls, account management, logging and monitoring of users

- sensitive information – handling

The methodology for the audit was consistent with and informed by the relevant Australian Standards for Assurance Engagements.

What Did We Find?

IT security policy

Three out of the five agencies tested did not have IT security policies. This is despite the fact that the agencies' IT systems were all storing personal and sensitive information regarding thousands of members of the WA public.

Without an appropriate IT security policy, staff may lack a basic understanding and awareness of the potential security risks for their IT environments. Staff may not be aware or have clearly defined their roles and responsibilities in managing those risks.

An IT security policy should be based on a detailed assessment of the potential threats and vulnerabilities to the IT systems, and guide procedures and controls to mitigate identified risks. The policy should also define senior management's commitment and approach for ensuring adequate safeguards and controls are in place to protect the confidentiality, availability and integrity of information. To ensure the requirement for effective information security is fully understood, the IT security policy should be readily available and communicated throughout the organisation.

Administrative controls

Agencies should have a number of simple administrative controls in place for staff dealing with personal and sensitive information. These include:

- Background screening and criminal record checks of all people who will have access to computer systems and personal and sensitive information.

- Signed non-disclosure/confidentiality agreements detailing individual responsibilities with regards information handling and disclosure.

- Signed IT acceptable use agreements detailing individual responsibilities with regards system and information access.

In two of the five agencies reviewed there was no requirement to carry out police and background checks on staff before they were employed and given access to sensitive information. In another agency, police and background checks had been conducted for only 20 per cent of the staff.

All of the agencies had established some of the above controls, which indicates they had considered risks and acknowledged the need for the controls. However, none of the agencies were consistently applying them. We found a number of instances where staff had not been subject to police checks or required to sign confidentiality or acceptable use agreements even though there was a clear requirement for them to do so.

Network security

Agencies use computer networks to store, share and communicate information. Information on agency networks can be shared both internally and externally for the general public. Networks need to be configured to define who is authorised to access different 'areas' of information storage as well as different types of computer applications.

Network controls provide a range of mechanisms which are critical to ensuring only authorised users can access the network and connect to applications and databases storing sensitive information. Examples of network controls are

● access and authentication – to prevent unauthorised users accessing the network

● account management – defining the areas of the network that authorised users can access and the associated privileges. Highest level privileges include the ability to create passwords and accounts and change network controls. Common privileges include the ability to create, edit or delete documents

● logging and monitoring of usage – enabling network administrators (those in charge of managing and oversight of the network system) to track who has logged on and off at what time as well as unsuccessful attempts to log on to the network

● software security updates – vendors of network operating software typically provide updates or 'patches' to address known security flaws and vulnerabilities.

Four of the five agencies had active network accounts belonging to former employees including former IT staff with the highest level privileges. Such accounts mean that individuals within the agency could access the network with malicious intent and virtually no risk of being personally identified. Where accounts have highest level privileges, a person within the agency could accidentally or deliberately alter all privileges to existing users as well as delete or alter information and do so with detection being almost impossible.

Generic accounts allow individuals to access networks without being identified. All of the agencies we examined had generic network accounts with over 1000 across the five agencies. Many of these had been assigned weak passwords that were easy to guess or did not require a password despite providing access to sensitive information.

In one agency a number of generic accounts had been provided with remote access to their network and main application. We were able to easily guess these account passwords, which then enabled full access to sensitive information on thousands of WA individuals via the Internet.

In another of the agencies it was an accepted practice to write down the details of generic accounts and passwords and stick the details on computer monitors. These accounts could have been used by non agency staff such as cleaners, building maintenance contractors or general visitors to gain access to sensitive information.

Three of the agencies did not have appropriate network audit logs in place to capture network access details. Effective logging and pro active reviews are a critical detective control in the identification of unauthorised access attempts or suspicious activity such as after hours log in.

Despite the well known risks to computer systems of not deploying vendor security updates to secure systems and reduce vulnerabilities, three of the agencies did not have an effective process in place to manage this. Our scans of their network environment identified key systems that were missing critical software security updates.

Computer applications and database security

Computer applications provide users with an interface to access, enter and retrieve information from databases. Similar to the controls that exist for computer networks, applications and databases have specific controls to prevent unauthorised access or to limit the ability of users to create, delete or edit information held in the database. As with network security, key application controls include:

- access and authentication – to prevent unauthorised users accessing the database

- account management – defines who can access the database and the level of 'privileges' assigned. Privileges can range from ability to alter the design and structure of the database to simple read access of data stored in the database

- logging and monitoring of usage – enabling database administrators to track who has logged on and off at what time as well as unsuccessful attempts to log on to the database

- software security updates – software vendors provide updates or 'patches' to address known security flaws and vulnerabilities in their applications including database applications.

We found a range of fundamental weaknesses in the applications and database controls across the agencies we examined. Specifically:

- Four of the agencies were not effectively managing the system application and database accounts and had active accounts belonging to users who no longer worked there. These types of accounts provide opportunities for misuse by insiders with minimal chance of tracing the individual responsible.

- Two agencies were storing sensitive information using database applications that were grossly inadequate for that purpose. The applications had no password controls and a well known security weakness which allowed the initial log on screen to be bypassed providing full access to all information.

- In two of the three agencies that used a specific system, they had left well known default database accounts active and still set to their default password. Database vendors warn that security is most easily compromised by leaving default passwords unchanged for these accounts.

Sensitive information handling

Even with adequate controls in place at key layers of the security model, if sensitive information is not handled appropriately, all the security can be bypassed and information exposed, lost or stolen. This is especially true now with the widespread use of portable media devices such as USB drives providing people with cheap and easy ways to store and transport large volumes of information.

Based on this risk we assessed whether any personal or sensitive information had not been appropriately secured and could easily be found and accessed. We also looked for any controls to prevent sensitive information being copied and removed from the agency.

Across four of the five agencies we found thousands of highly sensitive files and documents regarding members of the WA public saved to unsecured network folders. This information could be viewed by anyone connected to the network, copied to portable media and removed from the agency.

In recent years there have been a number of high profile cases in the United Kingdom and elsewhere of portable media containing personal and sensitive information being lost or stolen. Despite this, none of the agencies we examined had implemented adequate controls to mitigate this risk. In fact in most of the agencies the use of USB drives by agency staff was a common and accepted practice.

General Computer and Application Controls Audits

Overview

Computer controls can be defined as specific activities performed by people (manual) or by systems (automatic) to ensure confidentiality, integrity, and availability of computer systems is protected. Computer controls are often divided into two categories: general computer controls (GCC) that apply to computing systems as a whole, and application controls that apply to specific software programs or applications that run on the systems.

General computer controls audits

We further classify general computer controls into 12 generic categories. We rotate our review of these 12 cycles over three years. This year we focussed on five categories: management of IT risks, information security, business continuity, change control and physical security.

For the first time we are reporting the results of our work using capability maturity models. A capability maturity model is a way of assessing how well developed and capable the established controls are and how well developed or capable they should be. Capability maturity models were prepared for 41 of the 65 agencies examined. The models will provide a baseline for comparing results of our future GCC work.

Application controls audits

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 dependant 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 the five agencies.

We do not publically report the applications or agencies selected in our IS audits to minimise the risk they will be targeted to exploit reported weaknesses. In addition, our findings and recommendations are relevant across government and not just for the specific agencies selected.

Conclusion

We found multiple information system control weaknesses at the vast majority of the agencies we examined. These weaknesses have the potential to compromise the confidentiality, integrity and availability of the computer systems we examined.

Key Findings

General computer controls

Despite information system controls being a fundamental necessity to most government operations, we continue to find basic weaknesses across government. By continually failing to address theses weaknesses, agencies leave themselves vulnerable to computer system failures, unauthorised access to information, loss of information and fraudulent activity.

We reported well over 500 GCC related issues to agencies in 2008. Of the 41 agencies we assessed using the capability model, we found that:

- over 60 per cent had not established effective controls to manage IT risks, information security and business continuity

- 46 per cent of agencies had not established effective change controls

- 33 per cent had not established effective controls for management of physical security.

Application controls

Only one of the five business applications we reviewed was considered well managed with few control weaknesses. In total we identified 30 control weaknesses of which:

- Security weaknesses made up 50 per cent of the control weaknesses. These included computer vulnerabilities such as easy to guess passwords, unauthorised user accounts and failure to remove accounts belonging to former staff.

- Data processing controls issues made up 33 per cent of our findings. Weaknesses in data controls put the integrity of information processed at risk.

- The remaining 17 per cent of issues related to operations, change control and business continuity controls.

What Should Be Done?

- Policies and procedures – 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. 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.

GENERAL COMPUTER CONTROLS AUDITS

Background

General computer controls (GCC) include controls over the information technology (IT) environment, computer operations, access to programs and data, program development and program changes. We classify general computer controls into the following 12 generic categories:

- management of IT risks
- information security
- business continuity
- change control
- physical security
- systems software
- IT resource strategy and planning
- relationships with outsourced vendors
- database implementation and support
- network implementation and support
- information systems operations
- hardware support

The objective of our GCC audits is to determine whether the computer controls effectively support the confidentiality, integrity, and availability of information systems. The audits also involve assessing the adequacy of risk management and internal audit practices as they relate to computer processing environments.

We conduct three cycles of GCC audits each year. In the first cycle, we examine all agencies with a financial year end of 30 June which have computer environments classified by this office as dominant or significant. Our classification of computer environments considers volume of transactions that are performed and size and complexity of systems as well as the size of revenue and expenditure streams involved.

The second GCC audit cycle includes a review of all four Universities and the four metropolitan TAFE colleges. The six regional TAFE colleges are reviewed on a rotational basis covering two colleges each year. The Department of Education and Training (DET) is also reviewed each year as a provider of key accounting, financial management and student records systems for TAFE colleges. Although DET is the provider of these services, the TAFE colleges remain ultimately responsible for ensuring that adequate controls exist over the processing of their transactions.

The main purpose of the first two work cycles is to determine the level of confidence our financial auditors can place in the financial and performance information that they audit. In this way the IS Audit work both supports and influences the level of detailed financial audit work required to give overall assurance on the financial statements and performance information reported by agencies.

The third cycle of work involves high level GCC audits for a selection of 10 agencies not normally covered in the first two audit cycles. While these agencies generally do not have dominant or significant computer environments in terms of our normal criteria, they may have important systems when other factors are considered.

What Did We Do?

Each year we do a preliminary assessment of all 12 GCC categories at selected agencies to provide high level assurance that controls were appropriately designed and implemented. We also conduct tests of the reliability of the 12 control categories on a rotation bases over three years, though information security and change management are significant enough to audit every year. The results of the preliminary assessment can result in more categories being rotated in and can influence the amount of testing performed.

In 2008 we conducted GCC audits at 65 agencies. The categories we focused on were:

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

This review was undertaken in accordance with the Australian Standards on Assurance Engagements as issued by the Australian Auditing Standards Board with a view to providing reasonable assurance under those standards.

Capability maturity models

This year for the first time we are reporting the results from our use of capability maturity models. A capability maturity model is a way of assessing how well developed and capable the established IT controls are and how well developed or capable they should be. In 2008 we used the model at 41 of the 65 agencies where we conducted GCC audits. The models will provide a baseline for comparing results of our future GCC work.

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.

We used a five scale rating[2] listed below to evaluate each agency's capability and maturity levels in each of the GCC audit focus areas.

Rating criteria:

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 modeling 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.

---

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

We provided the 41 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.

What Did We Find?

More than 60 per cent of the agencies we assessed using capability models had not established effective controls to manage IT risks, information security and business continuity. Forty-six per cent of agencies had not established effective change controls and 33 per cent had not established effective controls for management of physical security. Figure 2 below represents the results of the capability assessments for the 41 agencies. Our expectations are that all agencies across the categories should be at least within the level three band.
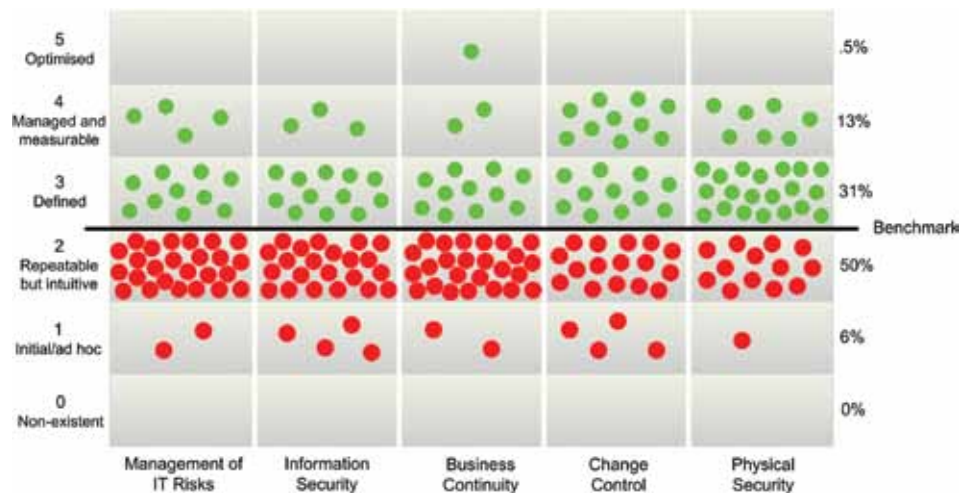
Figure 2: Capability Maturity Model Assessment Results

The model shows that most agencies achieved a rating of two or less out of five when assessed against each of the five GCC categories. The categories with the greatest weakness were Management of IT Risks, Information Security and Business Continuity.

36%

64%
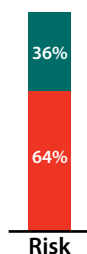
**Risk**

Management of IT risks

Treasurer's Instruction 825 Risk Management and Security requires all agencies to have risk management policies and practices that identify, assess and treat risks that affect key business objectives. The Treasurer's Instruction identifies IT as 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.

Sixty-four per cent of the agencies assessed using the capability model fell below our expectations for effectively managing IT risks.

Our general findings include:

- Some agencies either had no risk management policies and practices established or their policies and practices were inadequate.

- Most agencies have not analysed the likelihood and impacts of risk events.

- Many agencies do not maintain risk registers and lack clear processes for identifying and communicating risks. Agencies also lacked treatment plans and were not monitoring risks where they had been identified.

- Several agencies have not assigned responsibility to key staff for risk management. We found a lack of active participation by key staff across most agencies in the identification, assessment and treatment of IT risk management.

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.

39%

61%
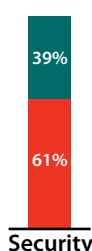
Security

Information security

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. We also examined whether only authorised software was installed on the agencies computer systems and used in accordance with licensing agreements and management's authorisation.

It is clear from the basic security weaknesses we identified that some agencies have not implemented fundamental security controls to secure their systems and information.

Sixty-one percent of agencies assessed using the capability model fell below our expectations for ensuring that information security is reasonably managed.

The information security controls we reviewed are divided into five main areas. The breakdown of findings across the five areas is shown in Figure 3 for all 65 agencies audited. The figure shows that weaknesses in access controls made up 46 per cent of security findings. Access controls are the most basic and inexpensive control to implement. Weaknesses with network security controls made up a further 26 per cent of our findings. Such weaknesses can leave information and systems on an agency's network vulnerable.
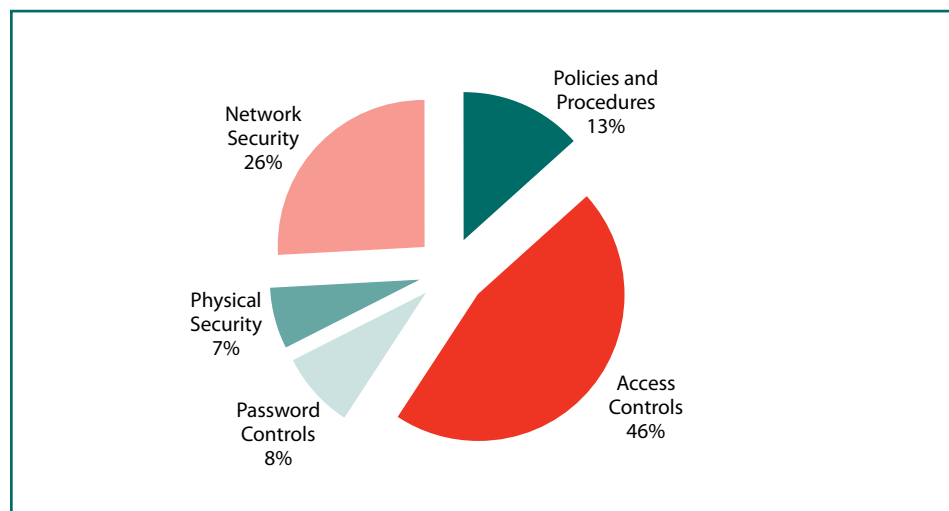
**Figure 3: Security Control Findings**

The graph shows that access controls and network security were the two most common types of security weakness amongst the 65 agencies.

Typical information security control weaknesses identified as part of the audit were:

- Critical files for payments to staff and external suppliers were stored on unsecured network folders allowing the files to be read and manipulated prior to processing.

- There was no segregation of duties for staff involved in financial processing and payment. This significantly increases the risk of fraudulent activity.

- Former employees with access to agency computer networks and applications increasing the risk of unauthorised access to agency resources and information

- Key systems had no password protection.

- There was no logging of user activity to identify and monitor who is accessing and making changes to agency networks, computer applications and database information, allowing security breaches to go undetected.

- Unsecured wireless access points provided open access to the agencies' internal network and systems

- Methods of managing devices on the network were insecure. This allows log on details such as user names and passwords to be easily intercepted, in turn leading to unauthorised and potentially undetected access to agency networks and information

- Agencies were unaware of the number of generic accounts that exist, who created them or who is authorised to use them. Generic accounts allow individuals to access networks without being identified

- Critical security updates were missing from computer systems and servers across agency networks. This leaves key systems and servers inadequately protected against potential threats and may result in unauthorised access and/or loss of system operation

- Agencies allowed uncontrolled installation of software on computers risking non-compliance with software licensing agreements and introducing a wide variety of threats. Threats include introducing viruses and spyware to the agency computer systems

- Financial and human resource databases had default user names and passwords unchanged. Attempting to log into computer systems and databases using default passwords is a common strategy used to gain unauthorised access to systems and information.

Without appropriate management of information security, there is a significant risk to the confidentiality, integrity and availability of information and computing resources.

Business continuity

36%

64%
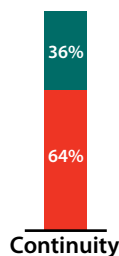
Continuity

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 that 64 per cent of agencies reviewed using capability models did not have adequate business continuity arrangements.

We identified the following issues relating to business continuity:

- agencies that had not conducted risk assessments or business impact analysis to inform and assist development of BCPs

- many instances of agencies not having tested, updated or developed adequate DRPs for the recovery of systems that support critical business functions and services

- inadequate backup testing for key network operating systems and data. This means that data could be permanently lost and systems could take excessive time to rebuild

- backup media stored in areas that do not provide sufficient protection against accidental or deliberate damage. This included backup media stored onsite and/or in unsecured areas

- several agencies had not tested uninterrupted power supplies (UPS). Without regular testing and maintenance of the UPS it is not possible to know if it will work in the event of a power disruption. We have seen several instances where the UPS have failed.

Without adequate planning for business continuity, there is an increased risk that key business functions and processes may not be restored in a timely manner after a disruption, in turn affecting the operations of an agency.

The lack of documented incident response procedures increases the risk that incidents may not be managed in a timely or effective manner particularly in the absence of key staff. Furthermore, required approval processes, escalations and critical systems can be overlooked in an emergency without clear incident response documentation.

Change control

54%

45%

Change

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.

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.

We found change control practices were not adequate in 46 per cent of agencies we assessed using the capability model. In some cases this has adversely affected agency systems and functions.

Common weaknesses we found included:

- no documented policies or procedures for how changes are to be made to key applications, databases and the IT infrastructure generally

- staff not aware that changes need to be approved and managed resulting in an ad hoc approach in some agencies

- agencies implementing significant changes to critical systems with no assessment of potential impacts

- no record of changes made to core systems and infrastructure. This means there is no up-to-date record of the current configurations needed to restore or fix critical systems if required.

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 unauthorised access given.

Physical security

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

67%

33%

Physical

We found inadequate physical security measures in 33 per cent of agencies we examined using the capability model. Common findings included:

- contractors and maintenance people with access to server rooms and equipment without management authorisation

- agencies not complying with their own policies for security over server rooms containing critical equipment

- agencies not recording or maintaining records of who has keys to server rooms containing critical infrastructure

- agencies locating vital network operating infrastructure such as routers and wireless access points in freely accessible areas

- server rooms lacking environmental controls such as temperature, humidity and smoke alarms, air conditioning and fire extinguishers

- server room doors left open or unlocked and unsecured server racks leaving network devices exposed to deliberate or accidental disruptions by individuals that enter the server room

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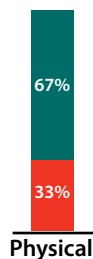
APPLICATION CONTROLS AUDITS

Background

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.

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:

- data entered into the application is accurate, complete and authorised

- data is processed as intended in an acceptable time period

- stored data is accurate and complete

- outputs, including online or hardcopy reports, are accurate and complete

- a record is maintained to track the process of data from input, through the processing cycle to storage and to the eventual output

- access controls are in place and user accounts are managed.

To gain assurance we review controls that directly affect the above processes. The control categories for application reviews are similar to those used for our general computer controls audits.

What Did We Do?

We reviewed five key business applications. Each application was selected on the basis of the significant impact on the agency or the public if the application was not managed appropriately. We assessed the adequacy of the controls for each application. The controls were:
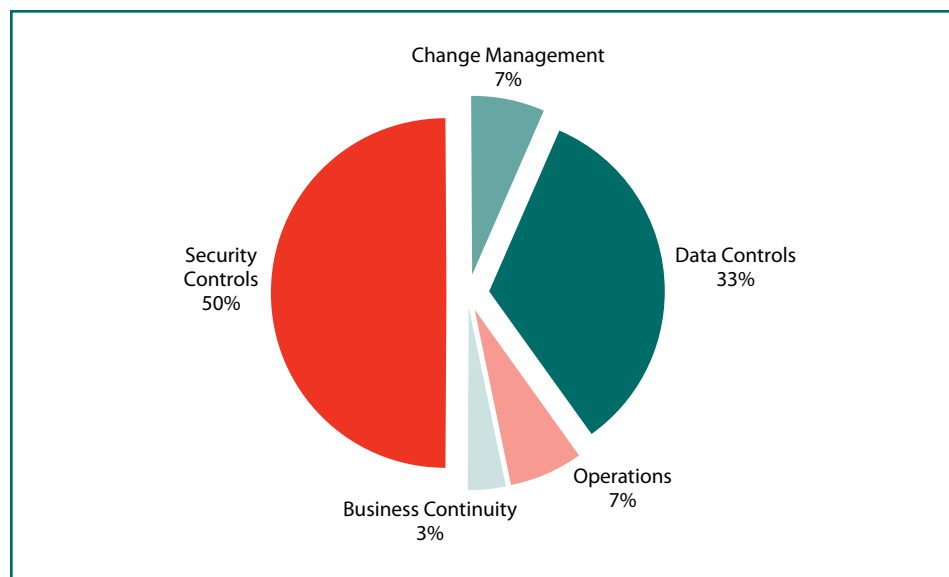
- security controls

- data controls

- operations

- change control

- business continuity

We do not publically report the applications or agencies examined in our IS audits to minimise the risk they will be targeted to exploit reported weaknesses. Another reason is that our findings and recommendations are relevant across government not just for the specific agencies examined.

This examination was undertaken in accordance with the Australian Standards on Assurance Engagements as issued by the Australian Auditing Standards Board with a view to providing reasonable assurance under those standards.

What Did We Find?

We identified 30 control weaknesses from the five business application systems reviewed. Security control weaknesses made up 50 per cent of the findings. Control weaknesses included computer vulnerabilities such as easy to guess passwords, unauthorised user accounts and failure to remove accounts belonging to former staff. Data processing controls issues made up 33 per cent of our findings. These weaknesses put the integrity of information processed at risk. The remaining 17 per cent of issues related to operations, change control and business continuity controls.

Figure 4: Application Control Findings

The graph shows that inadequate security controls and data controls were the two most common types of control weakness found in the five applications.

Security controls

We assessed whether security controls were implemented, administered and appropriately configured to restrict access to application data and related information.

The security weaknesses we identified put at risk the confidentiality and integrity of information processed by the applications.

Security controls weaknesses identified included:

- One application had no controls to prevent all users from viewing or accessing credit card details for members of the public. In addition there was no logging of activity to detect whether this was occurring, how often and by whom.

- One of the applications had inadequate security controls to prevent confidential client information being intercepted when transferred internally or via the Internet. This information could be used for unauthorised access and transactions .

- One agency had not defined the access privileges that should be applied for new staff resulting in inappropriate levels of access being assigned to numerous users. One agency was unable to produce a list of user accounts and their access privileges for an application.

- Active user accounts belonging to former staff and staff on extended leave were found at two agencies.

- In two applications we found numerous user accounts had been created without approval. These accounts allowed modification, addition and removal of information and user accounts. At one agency the accounts allowed access to highly personal information and in another agency to the processing of payments.

- Two agencies had not checked whether external parties connecting to their applications had appropriate security controls to prevent compromising computer systems.

- Critical security updates were missing from key applications in three agencies. This leaves the application inadequately protected against potential threats and may result in unauthorised access and/or loss of system operation.

Data controls

Prior to examining data controls for an application we obtain an understanding of the business processes involved and the underlying IT systems. We identify all relevant business and control activities and map the flow of information from input to output. This includes reviewing any policies and procedures as well as interfaces between applications.

We identified the following issues relating to data controls:

- In two applications the agencies had not formalised the types of controls that should be established over data processing. These should be formalised through approved policies and procedures.

- In two applications unauthorised staff were able to override controls and waive customer fees for services without being detected.

- Two agencies were not conducting routine verification of data accuracy and validity.

- Records transferred from one application to another were not checked to ensure completeness and integrity. This occurred both within an agency and between two other agencies.

- One application had no controls to ensure delays in processing, caused by incomplete or invalid data, were consistently followed up and resolved in a timely manner.

- One agency was manually processing data that could have been processed using their existing computer application. Use of the application would be more efficient and reduce the likelihood of errors.

- One of the applications had weak password protection that was easily bypassed allowing undetectable changes that would potentially compromise the validity of all fees calculated using the application.

Other control categories

Operations controls ensure that applications are used consistently and correctly across an agency to meet business requirements. These controls include staff training, application specific manuals, as well as monitoring and reporting of data input, processing and output.

Change control is required to ensure that any modifications to existing computer systems are appropriately implemented and changes are authorised, approved and tested where appropriate.

Business continuity planning is vital for all agencies as it provides for the rapid recovery of computer services in the event of an unplanned disruption.

In general these controls were adequate across two of the five applications. Nevertheless we identified a number of necessary improvements. These included:

- One of the applications did not have any design documentation making it difficult and expensive to maintain.

- In two agencies users of key applications had not received appropriate support and training in use of the applications.

- One agency had no documented policies or procedures for how changes are to be made to key applications, databases and the IT infrastructure generally.

- In three agencies changes were being made to key systems without being tested, recorded or authorised.

- One application did not have a disaster recovery plan. Without this the agency could not meet its own requirements for business continuity.

Reports of the Auditor General

2009

Public Sector Performance Report 2009   3 December 2008
– Management of Water Resources in Western Australia – Follow-up
– Administration of the Metropolitan Region Scheme by the
   Department for Planning and Infrastructure
– Management of Fringe Benefits Tax

2008

Second Public Sector Performance Report 2008   3 December 2008
– Complaints Management in Shared Service Centres
– Funding and Purchasing Health Services from Non-Government
   and Not-For Profit Organisations
– Management of Traffic Infringements for Government Vehicles and Staff

Responding to changes in attraction, retention and achievement in
Vocational Education and Training   12 November 2008

Audit Results – Assurance Audits completed at 3 November 2008
– Opinions of Ministerial Notifications   12 November 2008

Improving Resource Project Approvals   7 October 2008

The Juvenile Justice System: Dealing with Young People under the
Young Offenders Act 1994   18 June 2008

Lost in Transition: State Services for Humanitarian Entrants   11 June 2008

Audit Results Report on Universities and TAFE Colleges and
other audits completed since 19 November 2007 and
Performance Examinations of Risk Management, Delegation of Authority
and Records Management   7 May 2008

Public Sector Performance Report 2008   19 March 2008
– Regulation of Security Workers
– Information Security: Disposal of Government Hard Drives

2007

Renewable Energy: Knowing What We Are Getting	28 November 2007
Audit Results Report by Ministerial Portfolios at 19 November 2007 – Opinions on Ministerial Notifications – Administration of Natural Resource Management Grants	28 November 2007
First Do No Harm: Reducing Adverse Events in Public Hospitals	17 October 2007
Fourth Public Sector Performance Report 2007 – Management of Asbestos-Related Risks by Government Agencies – Tracking Timber Logged From South-West Native Forests – Establishing Contractual Arrangements with Private Business	26 September 2007
Management of Native Vegetation Clearing	5 September 2007
Third Public Sector Performance Report 2007 – Management of Land Tax and Metropolitan Region Improvement Tax – Legal Aid in Western Australia – The Administration of Grants	27 June 2007
A Helping Hand: Home-based Services in Western Australia	27 June 2007
Shared Services Reform: A Work in Progress	13 June 2007
Audit Results Report – Universities and TAFE Colleges – Other audits completed since 16 October 2006 – Legislative Changes and Audit Practice Statement 2007	4 April 2007
Second Public Sector Performance Report 2007 – Major Information and Communications Technology Projects – Security of Wireless Local Area Networks in Government	4 April 2007
Public Sector Performance Report 2007 – Arrangements for Managing the Performance of Chief Executive Officers – Prompt Payment by Government – Management of Consumer Protection Investigations	28 March 2007
Having Your Say: Public Participation in Government Decision-Making	28 February 2007

**The above reports can be accessed on the Office of the Auditor General's
website at www.audit.wa.gov.au**

**On request these reports may be made available in an alternative format
for those with visual impairment.**