CONTENTS

Western Australian Auditor General's Report

# Information Systems Audit Report

Report 4 – June 2011

**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
15 June 2011

# Contents


## Auditor General's Overview 4

## Cyber Security in Government Agencies 5

## Application and General Computer Controls Audits 16

### Application controls 19

### General computer controls and capability assessments for agencies 25

# Auditor General's Overview

The Information Systems (IS) Audit Report is tabled each year by my Office. This is an important report because it identifies a range of common IS issues that can seriously affect the operations of government if not addressed.

The report has two sections covering three items:

- Information Systems performance audit
  - Cyber security in government agencies
- Application and general computer controls audits
  - Application controls audits
  - General computer controls and capability assessments of agencies

The first item of the report, 'Cyber security in government agencies', looked at agencies ability to detect and respond to cyber threats. Such attacks can impact on the availability, confidentiality and integrity of agency computer systems. The audit identified significant vulnerabilities to cyber threats in all 15 agencies examined.

The second item of the report contains the results of our audit of five key business applications at five agencies. We found weaknesses in security and data processing controls that could potentially impact delivery of key services to the public.

The third item contains the results of our general computer control audits conducted at over 40 agencies. It shows that there has been no overall improvement in agency controls over their computing systems in the last year with a high proportion of agencies still not meeting our benchmarks.

Our work highlights that agencies often struggle to keep up with constantly changing issues and risks with information technology systems and security. Agencies often work independently of each other, despite facing similar challenges. There is an opportunity for greater coordination across government in the area of information technology, standards and guidance for agencies.

# Cyber Security in Government Agencies

## Overview

Western Australian government agencies rely heavily on the Internet to deliver services and conduct business. However, operating in cyberspace carries serious security risks to agency information and systems that need to be mitigated. The cyber security threat is no longer an emerging threat – it exists now and the risk is growing.

An agency's connection to the Internet exposes its information and systems to exploitation from anywhere in the world. The Internet also provides information about how to identify network vulnerabilities and how to exploit them. It is even a source of freely available tools that can be used to exploit weaknesses.

The challenge to agency chief executive officers is clear – recognise the risk and take appropriate precautions to protect their confidential information and systems.

Most agencies maintain a wide range of confidential information that has potential value and needs protection. For instance, information about actual and proposed government business plans, commercial-in-confidence information provided by the private sector during contract negotiations, and personal details of employees and private individuals that in bulk form in particular has potential commercial value.

Accessing confidential information is not the only motivation for cyber security threats. Some security threats are motivated by mischief or worse and can result in systems being damaged or shut down.

Often employees are the weakest link in security of information systems. The 'internal threat' of employees knowingly or unknowingly compromising computer systems is an issue that agencies need to recognise and manage.

This audit assessed whether 15 agencies had configured their IT systems and had supporting policies and processes in place to detect, manage and appropriately respond to cyber attacks.

We conducted benign cyber attacks on the 15 agencies via the Internet. We also scattered USB devices across the agencies to test agency staff. The devices contained software that would 'phone home' and send network specific information across the Internet if plugged in and activated.

## Conclusion

None of the agencies we tested had adequate systems or processes in place to detect, manage or appropriately respond to a cyber attack. Only one agency detected our attacks. The failure of most agencies to detect our attacks was a particular concern given that the tools and methods we used in our tests were unsophisticated.

## Key Findings

- Fourteen of the 15 agencies we tested failed to detect, prevent or respond to our hostile scans of their Internet sites. These scans identified numerous vulnerabilities that could be exploited to gain access to their internal networks and information.
- We accessed the internal networks of three agencies without detection, using identified vulnerabilities from our scans. We were then in a position to read, change or delete confidential information and manipulate or shut down systems. We did not test the identified vulnerabilities at the other 12 agencies.
- Eight agencies plugged in and activated the USBs we left lying around. The USBs sent information back to us via the Internet. This type of attack can provide ongoing unauthorised access to an agency network and is extremely difficult to detect once it has been established.
- Failure to take a risk-based approach to identifying and managing cyber threats and to meet or implement good practice guidance and standards for computer security has left all 15 agencies vulnerable:
  - Twelve of the 15 agencies had not recognised and addressed cyber threats from the Internet or social engineering techniques in their security policies.
  - Nine agencies had not carried out risk assessments to determine their potential exposure to external or internal attacks. Without a risk assessment, agencies will not know their exposure levels and potential impacts on their business.
  - Seven agencies did not have incident response plans or procedures for managing cyber threats from the Internet and social engineering.
- Nearly all the agencies we examined had recently paid contractors between $9 000 to $75 000 to conduct penetration tests on their infrastructure. Some agencies were doing these tests up to four times a year. In the absence of a broader assessment of vulnerabilities, penetration tests alone are of limited value, as our testing demonstrated. Further, they are giving agencies a false sense of security about their exposure to cyber threats.

## What Should Be Done

Agencies should:

- identify and manage information security risks. Information security risks need to be managed within an overall risk management framework.
- ensure they have appropriately configured mechanism(s) for detecting cyber threats from the Internet. In particular, agencies should configure their systems to protect themselves against hostile and freely available tools.
- perform regular information security awareness training for staff, including the risks associated with the Internet and social engineering.
- ensure they have a good understanding of the services being provided by security consultants, and the extent to which these services provide assurance against identified risks.

# Agency Response

## Fremantle Port Authority

This audit has been worthwhile and has highlighted a number of issues. Implementing measures to address these issues will improve Fremantle Ports' security against potential internet based attacks and increase staff awareness of these potential threats.

## Legal Aid WA

The report highlights the constantly changing nature of information security threats and the need for agencies to remain vigilant in order to reduce the risk posed by cyber threats. The findings provide valuable input into the continuous process of testing and improvement that is necessary for our security systems and processes to be effective.

## Department of the Attorney General

The Department of the Attorney General welcomed the opportunity to participate in this examination, as it provided an independent external review of the Department's information system controls in relation to cyber threats. The findings and recommendations presented in this report are relevant and will be examined as a priority by the Department.

## Department of Education

The Department agrees with the findings of the audit report and will undertake staff training in security awareness. In addition, the Department's Security Incident Response plan will be refined to address the escalation issues. The Intrusion Detection issues relate to a technical capacity limit with the hardware and have since been addressed.

## Department of Health

The Department of Health takes seriously and acknowledges the recommendations made by the Office of the Auditor General and has taken immediate steps to reallocate funding and has undertaken immediate planning to ensure that WA Health has a more robust and appropriate ICT Security framework. To ensure the recommendations are addressed in an appropriate timeframe, three target areas will be addressed simultaneously.

## Main Roads

Main Roads agrees to review our current security threat processes and products and produce an action plan to address all the issues raised from this audit. This action plan will detail what changes will need to be made to settings and/or processes, and if necessary what new software and/or hardware will need to be purchased.

## Department of Transport

The Department of Transport (DoT) has completed a detailed analysis of vulnerabilities to the external facing network and the internal network. The strategy DoT adopted was to do a detailed analysis and develop a vulnerability matrix, unlike doing penetration tests, which would give DoT a false sense of security about the exposure to cyber threats. Implementation of some of Audit's recommendations has already commenced.

## Synergy

Synergy considers its core servers and systems to be well protected from cyber attack. Notwithstanding this, Synergy welcomes feedback provided by the OAG audit, as it allows us to improve existing measures to address the constantly changing threat of cyber crime.

## Landgate

Landgate has considered the findings in the audit and has undertaken or has scheduled appropriate measures to mitigate the risks identified.

## Lotterywest

Lotterywest welcomes any audit which has the potential to strengthen our defences in the internet sphere. We have set up our web security in a way which takes into account the very high level of traffic which our very popular site receives on a day to day basis. Our security systems have been tested by external specialists in this area and to date found to provide adequate protection to ensure the integrity of our systems. We continue to work with the OAG's office to explore ways in which this audit can assist us in the commitment of Lotterywest to ensure that our systems integrity remains of the highest order.

## ServiceNet (Department of Treasury and Finance)

The Department of Treasury and Finance acknowledges the findings of the audit and is working actively to ensure that its processes and technology is upgraded to improve protection against cyber security threats. A number of the items identified in the audit have already been addressed and have already been closed out.

## Department of Mines and Petroleum

The Department of Mines and Petroleum (DMP) has been taking direction from the Department of Defence and, to a lesser extent, the former Office of e-Government in developing its IT security framework and determining IT security priorities. DMP acknowledges the findings of this report, will modify its IT security prioritisation framework to accommodate OAG's feedback, and work towards improving the shortcomings identified. It will also attempt to work with the Public Sector Commission and the Inter-Agency Information Security Management Group towards establishing a more consistent security framework across both State and Commonwealth governments.

## Background

Most if not all government agencies have an Internet presence. The Internet acts as a 'shopfront' for agencies, allowing them to communicate with the public. The public typically use the Internet to pay for government services such as electricity, water, gas and various licences. They also use the Internet to seek information from government. This ease of access to services and information through the Internet has many benefits.

Despite the many benefits, an Internet presence exposes agency computer systems to 'cyber attack' from anywhere in the world. This is because the Internet is usually directly connected and can act as a gateway into an agency's internal computer networks. While the Internet is a form of electronic shopfront for agencies, their internal computer networks can be considered the 'warehouse'. Internal computer networks store and process data that is essential in the day-to-day functioning of the agency. Some of this data can be sensitive.

The risk is real and while most attacks will probably go unnoticed or unpublicised, there have been a number of high profile cyber attacks in Australia and overseas recently that have received publicity. These attacks have compromised business computer networks and in some cases sensitive information has been stolen.

Countries such as the United Kingdom and the United States have mandatory reporting requirements that compel business and government to disclose if their systems have been compromised. Such requirements help to focus management attention on information security. There are no mandatory reporting requirements in Australia.

A risk less often considered to an agency's computer networks is the risk of attack from within. This can occur through a disgruntled employee or through 'social engineering' where an attack relies on for example, an employee's curiosity to plug in a USB device left lying around. The USB can contain software that provides access and/or collects and sends information back out through the Internet to the cyber attacker.

The following diagram represents a simple architecture for an agency with an Internet site.

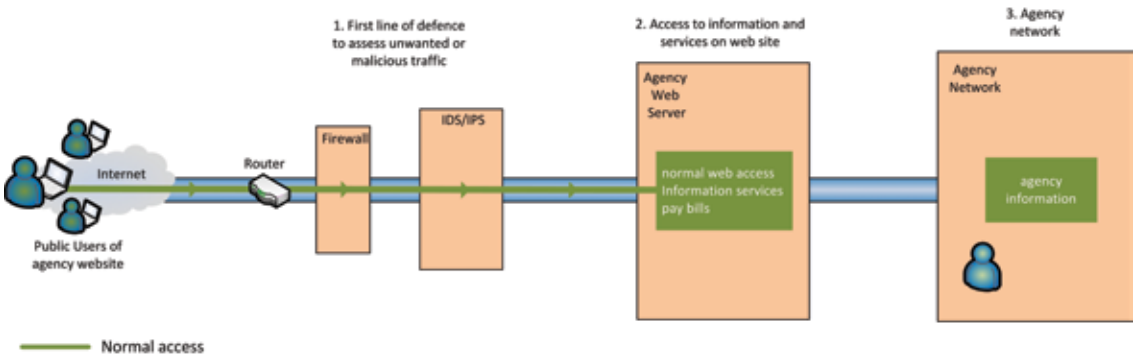



**Figure 1: Shows how an agency's web server provides potential connection through to its internal computer networks. A properly configured Firewall and IDPS are essential to protect agencies from cyber threats.**

The Internet provides global access to an agency's web site. The web site is usually on a separate computer or a 'web server'. The web server can be directly managed by the agency or by a third party such as an Internet Service Provider (ISP). The agency usually needs to be connected to the web server to process transactions generated by users and to update web site information. Agencies often use the same infrastructure to process emails going into and out of the agency. Because of this there is a continual two-way flow of information traffic into and out of an agency's network to the Internet.

The first line of defence against a cyber attack through the Internet is the ability to detect and prevent suspicious or malicious traffic. Generally this would be done through a combination of a Firewall and an Intrusion Detection/Prevention System (IDPS).

The firewall will permit or deny network traffic based on a set of rules configured by the agency. A firewall is a bit like a traffic policeman who has been instructed to only allow certain types of cars to pass backwards or forwards across a bridge.

An IDPS is more like a border control guard, who is on the look out for suspicious goods and will search the car before it is allowed to go across the bridge. An IDPS monitors network and system activity to identify traffic that is known or suspected to be malicious. The IDPS can be configured to automatically prevent certain types of traffic or to signal to a system administrator that suspicious activity is occurring.

Agencies have a responsibility to ensure the security of their computer networks. Information security standards and good practice guidance can assist agencies in this task.

## What Did We Do?

We assessed whether agencies had configured their IT systems and had supporting policies and processes in place to be able to detect, manage and appropriately respond to cyber attacks. The key questions we asked were:

- Has the agency conducted risk assessments for cyber threats?
- Is there a security policy and/or framework that consider cyber threats?
- Are controls in place to effectively detect and manage cyber intrusions?
- Are incident response plans and recovery processes in place?

The agencies selected for this examination were:

- Department of the Attorney General
- Department of Education
- Department of Health
- Department of Mines and Petroleum
- Department of Transport
- Fremantle Port Authority
- Gold Corporation
- Landgate
- Legal Aid
- Lotterywest
- Main Roads
- ServiceNet (provision of Internet and web server hosting for many agencies)
- Synergy
- Water Corporation
- Western Power

In conducting our audit we took precautions against inadvertently compromising information held on agencies internal computer systems and the risk that our attacks could seriously impede performance or 'crash' agency computer systems. For example, where agencies had large and complex computing environments and provided critical services, we advised senior management of the testing we were going to perform. This enabled them to advise us of any foreseeable risks. They were asked not to inform the staff directly responsible for detecting and responding to incidents, and not to assume any detected activity was necessarily from the audit office. The remaining agencies were advised more generally that we would test their ability to detect and respond to threats that arise in their computing infrastructure and networks.

We also worked closely with the Police Technology Crime Investigation Team. This team handles investigation and response when a potential cyber attack (unauthorised use) is reported. Unauthorised use of computer systems is a criminal offence under the Criminal Code.

Prior to commencing the audit at agencies we reviewed their policies and procedures for identifying and responding to cyber threats. This included reviewing information security policies, incident response plans, staff induction processes, and security awareness training.

We performed external and internal attacks to test the vulnerabilities of agency computer systems.

## External attack

We engaged the Security Research Centre at Edith Cowan University (ECU) to conduct the external 'attacks'. We did not provide ECU with any information on agency networks. They were required to seek our approval before attacking any specific IP addresses they identified at agencies. This enabled us to guide ECU in their testing to ensure they did not attack computers that hosted key services.

Our external attack was done in two stages. The first stage undertaken on all 15 agencies was a scan of agency Internet sites using publically available scanning software downloaded free from the Internet. The software is typically used by network administrators to run internal security scans to identify weaknesses and follow up any exceptions and problems.

These preliminary scans were deliberately hostile (prolonged and continuous) in a best effort to have our activity detected without making the test a Denial of Service (DoS). A DoS attack is a concerted effort to degrade or prevent the functioning of an Internet site or service by bombarding the server with traffic.

The second stage of our attack was undertaken at three agencies and used information gained from the scan to exploit identified vulnerabilities. We did this to prove the vulnerabilities and to demonstrate the sort of information that could be accessed.

### Internal attack

Internal weaknesses arise through lack of awareness of potential threats and inadequate policy and process to deal with these threats. An example of this is allowing employees to plug non-agency USB devices (USBs) or other devices into internal networks.

We deployed 25 USBs across 15 agencies. At 12 agencies the USBs were left in public access areas such as reception or cafeterias. At another three agencies the USBs were left within the agency premises in areas not normally accessible by the public. We recorded when and where each of the USBs were deployed.

These USBs did not contain auto-executing malware but instead relied on a social approach. An individual would have to pick up the USB, plug it in, then make the decision to read a file and then run a program. The message contained within the file and the steps required to run the program should have been sufficient to make an individual suspicious and wary. If activated, the USB was designed to 'phone home' telling us where it was and sending some basic network information.

On completion of our attacks, we debriefed agencies with our specific findings. We also requested log files to determine whether the agencies had logged our activity. Log files are essential in the case of a real cyber attack as part of the evidence required by Police to support a prosecution.

We conducted the audit in accordance with Australian Auditing Standards

## What Did We Find?

None of the agencies we tested had appropriate systems or processes in place to detect or respond to a cyber attack. Figure 2 summarises the access we achieved with our attacks. It illustrates the serious weaknesses in computer security at the agencies we tested.

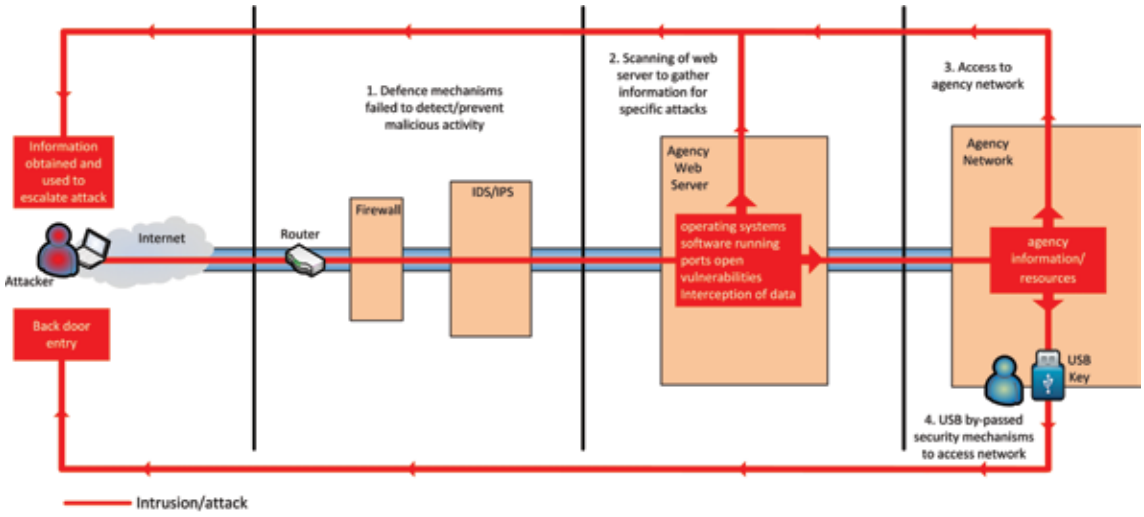



**Figure 2: Access gained by audit to agency computer systems**

## Fourteen of fifteen agencies failed to detect, prevent or respond to any of our hostile scans.

We used freely available software from the Internet to run scans on agency web servers. Fourteen agencies did not detect this activity even after repeated scanning and probing. The scans identified numerous vulnerabilities that could be used to conduct more specific attacks to gain access or control over agency systems.

We were concerned about the lack of detection of our scanning by agencies in general. In some cases we chose to escalate the attacks in a specific attempt to have our activity detected. For example, at one agency we conducted a 'brute force' attack that made several million attempts to gain access to a web server. We noticeably degraded the performance of the agency's network without denying user services. However despite this, the attack went unnoticed by the agency. This was even more concerning given that this agency had specifically engaged a contractor to identify cyber threats.

Appropriately configured firewalls and IDPS should detect and automatically prevent such scanning. They should also prevent any information being returned to the source of these scans. In addition, web servers should be configured to prevent technical information from being collected from a scan.

However, we found this not to be the case. All of the agency web servers allowed technical information to be collected, and poorly configured firewalls and IDPS failed to prevent this information being returned to the source of our scan. This information included the operating system and version, the type of firewall in use, and what software was running. This information could then be used to determine vulnerabilities and methods to exploit them.

The ability to detect, prevent and respond to scans from the Internet is important for ensuring that a cyber threat can be appropriately handled in a timely manner. A deceptive scan or attempt to access the agency's network is unlikely to be detected by these agencies. It is possible for an average user to download software to enumerate an agency's network in order to gain unauthorised access or cause disruption to business functions.

## We accessed the internal networks of three agencies without detection

We selected a very small sample of potential vulnerabilities returned from the scans of three agencies and used them to access the internal networks of these agencies. This was done without detection. Of significant concern was that we gained access without the need to undertake any detailed analysis of the scans to determine all of the potential vulnerabilities that existed.

In one agency we obtained several usernames and passwords for databases in their networks. In another we accessed the login screen for web administration systems. This access could have been used to intercept credit card transactions. In a third agency we gained access to internal network folders to view and copy information.

Based on the ease of access at these three agencies, it is highly likely that we could have accessed the internal computer networks and information at all the agencies in our sample if we had chosen to.

## Eight agencies plugged in and activated the USBs we left lying around

USBs we left lying around at eight agencies were plugged into agency networks and activated. The USBs then 'phoned home'. While our USBs did not pose a threat to the agency networks, the exercise clearly demonstrated how this type of attack can provide unauthorised access to an agency network. Significantly, it is also extremely difficult to detect once it has been established.

Eight of the 15 agencies had their network compromised by USBs that we left at agencies to test their security practices. The USBs were found by agency staff and subsequently connected to their agency's networks. This exercise proved how easily existing security mechanisms can be undermined if staff are not properly trained. It is also a highly dangerous form of attack because it allows a perpetrator to gain direct access into the agency's network, thereby providing control over information resources from the Internet without detection.

Of the remaining USBs we deployed:

- three agencies found them and reported them internally as lost property
- several USBs found their way into home computers or the networks of private organisations and were plugged in. As previously mentioned, they posed no threat and the software contained within them could be easily deleted.

This aspect of our audit highlighted how important it is that agencies manage all the potential risks to their systems. Agencies can address this particular risk through staff training. Software can also be used to prevent or manage unauthorised USBs or other devices from being connected to their networks.

## Agencies lack a risk based approach to computer security

The results of our audit highlight that agencies are not taking a risk-based holistic approach to managing the security of their computer systems. They are failing to meet good practice guidelines and standards for computer security.

We reviewed the policies and procedures of agencies to assess how well they have identified potential risks to their networks and what controls are in place to manage those risks. We found that 12 of the 15 agencies had not considered cyber threats from the Internet or social engineering techniques in their security policies.

Nine agencies had not carried out risk assessments to determine their potential exposure to external or internal attacks. Without a risk assessment, agencies will not know their exposure levels and potential impacts on their business.

Seven agencies did not have incident response plans or procedures for managing cyber threats from the Internet and social engineering. Staff did not know how to respond to cyber threats and under what circumstance they should escalate.

Twelve agencies did not provide information security awareness training for their staff. Employees can pose the biggest risk to information security and bypass all other security mechanisms. This weakness can undermine the security requirements for agencies and lead to the compromise of systems.

Many agencies had a false sense of security about their protection from cyber threats. For example, nearly all agencies we examined had recently paid contractors between $9 000 to $75 000 to conduct penetration tests on their infrastructure. Some agencies were doing these tests up to four times a year. These tests conducted in isolation are of limited value, as our testing demonstrated.

A number of agencies had paid third party service providers and contractors to manage their cyber security. However, our tests proved this management was ineffective.

Agencies need to conduct proper assessments that identify and test all vulnerabilities including people, processes, technology and data. A useful reference is the Department of Defence *Strategies to Mitigate Targeted Cyber Intrusions*. This includes 35 strategies that agencies can consider for protecting their network environments.

# Application and General Computer Controls Audits

## Overview

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

### 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 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 five agencies.

### General computer controls and capability assessments of agencies

We focused on five general computer control categories: management of IT risks, information security, business continuity, change control and physical security.

We use capability maturity models in conjunction with our GCC audits to help report the results of our work. 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 assessments were prepared for the 46 agencies audited. The models provide a benchmark for agency performance and a means for comparing results from year to year.

## Conclusion

We were encouraged to see one agency had good controls in place for a key business application we reviewed. However all of the other agencies we reviewed in our application and general computer controls audits had multiple information system controls weaknesses. It is disappointing that signs of improvement from last year have not been sustained.

# Key Findings

## Applications controls

Four of the five business applications we reviewed had control weaknesses though change management and business continuity controls were reasonable and operational controls were strong. In total, we identified 18 control weaknesses of which:

- Security weaknesses made up 67 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 22 per cent of our findings. Weaknesses in these controls put the integrity of information processed at risk.
- The remaining 11 per cent of weaknesses related to business continuity and change management issues such as untested disaster recovery plans and unauthorised changes to key applications.

## General computer controls and capability assessments for agencies

Our capability assessments showed no overall improvement from last year in the management of general computer controls by agencies. Specifically:

- Fifteen per cent of agencies we reviewed last year using the capability assessments regressed in at least one area without making any improvements.
- Forty-three per cent of agencies showed no change.
- Another 15 per cent made improvements in at least one of the categories without regressing in any category.
- Six per cent moved up in one category but went down in another.
- Twenty-one per cent of agencies were assessed for the first time.

Sixty-four per cent of the agencies we assessed using capability models had not established effective controls to manage IT risks, information security and business continuity. Thirty-three per cent of agencies had not established effective change controls and 37 per cent had not established effective controls for management of physical security.

We reported 381 general computer controls related issues to agencies in 2010. Three per cent of these issues were rated as significant, requiring immediate attention. Sixty per cent were rated as moderate, requiring attention as soon as possible.

The results of our work highlight the need for agencies to maintain a continued focus on their information systems controls.

## What Should Be Done?

Poor controls over business applications create serious exposures and can lead to the compromise of information stored and handled by agencies. Agency management relies on accurate information from their business applications in order to make informed decisions. Agencies need to have appropriate controls in place to ensure the complete and accurate processing of data from input to output. Specifically agencies need to continually focus and assess the adequacy of the following controls over their business applications:

- 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.

# APPLICATION CONTROLS

## Background

Each year we audit a selection of key applications that are essential to government operations. Failings or weaknesses in these agency applications have the potential to directly impact other agencies and/or members of the general public. Impacts range from delays in service to possible fraudulent activity and financial loss.

## What Did We Do?

We reviewed one key business application at each of five agencies. Our audit involved an in-depth focus on the step by step processing and handling of data. Our objective was 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.

This year we reviewed the following agencies and applications:

### Department of Treasury and Finance (Office of Shared Services – eBusiness)

The Office of Shared Services' main application is eBusiness. This application handles financial transactions for more than 60 agencies as part of a Shared Services arrangement.

### Landgate (SLIP – Shared Land Information Portal)

SLIP delivers online real-time access to spatial information. This information is used by government agencies the public and private entities for planning, land use and development, environmental sustainability and emergency management. SLIP combines a number of databases and applications that enable users to access and research WA land and geographic resources online.

### Government Employees Superannuation Board (Capital)

The Capital system is used to manage the superannuation funds of WA Government employees including contributions, payouts and balance sheet liabilities for agencies and employees. The system depends on transfers of information from agency payroll and personnel systems. Fund members can access the system over the internet to change their superannuation investment profiles.

### Department of Fisheries (FLAMS – Fishing Licensing and Management System)

FLAMS is a commercial and recreational fishing licensing system. It handles a significant number of financial transactions over the Internet for new and renewed Western Australian commercial and recreational fishing licenses. FLAMS also records and helps manage information on licence restrictions, quotas for commercial fishers and associated personal information.

### Police (SAP – Enterprise Resource Planning System ERP)

SAP is the enterprise resource management system used by the WA Police. Its key functions include human resource and financial management.

## What Did We Find?

We identified 18 control weaknesses in four out of the five business application systems reviewed. Only the Police's SAP application had good controls for each of the areas we reviewed.

Security controls weaknesses were the main concerns in the other four applications, making up 67 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 control issues made up 22 per cent of our findings. These weaknesses put the integrity of information processed at risk. The remaining 11 per cent of issues related to change management and business continuity with no issues reported for operations.

Figure 3 summarises our findings against each of the agencies applications.

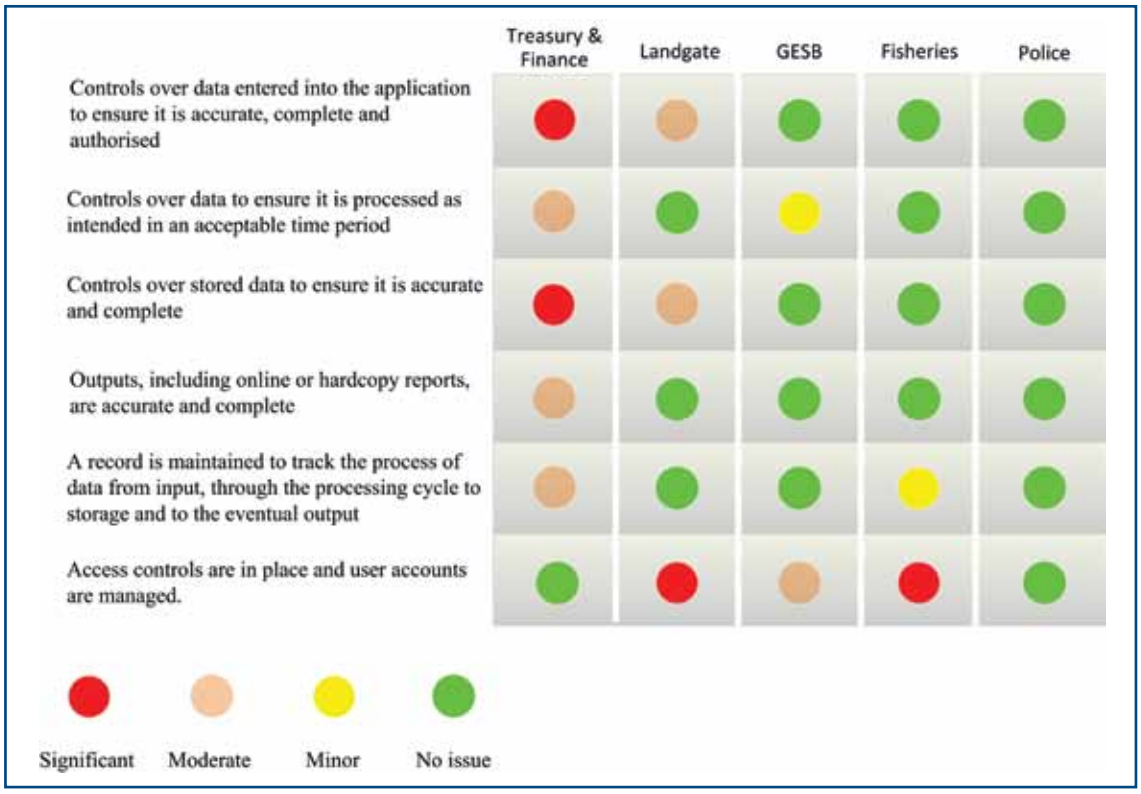



**Figure 3: Summary of findings for each business application. The Department of Treasury and Finance's eBusiness application at the Office of Shared Services had significant control weaknesses in two key areas. These weaknesses flowed into other control aspects of the application.**

## Department of Treasury and Finance (Office of Shared Services – Finance System)

We found control weaknesses over data being uploaded into the eBusiness application. These weaknesses create a risk that the data uploaded may not be accurate, complete or authorised. Existing file transfer protocols within the Oracle business solution have been overlooked in favour of developing customised solutions for transfer of data files from agencies. These customised solutions do not include any data verification controls. As a result, incomplete and erroneous data and duplicates can be loaded into the database.

The lack of data verification also means stored financial data and any reports generated from the system are at risk of being inaccurate and incomplete. We also found that when the customised interfaces experience technical difficulties this increases the time taken to process data. In addition, there are significant backlogs in data that need to be processed manually.

Customisation of interfaces means that future software upgrades may not be supported without significant development activities and cost.

## Landgate (SLIP – Shared Land Information Portal)

We found controls over the accuracy and completeness of stored information were inadequate. Data updates are sourced automatically from various agencies. However SLIP has no mechanism to check that the updates have completed successfully and that the data is accurate and complete. The agency is relying on end users to inform them of errors and incorrect information. This may mean information the public and other government agencies are relying on could be incorrect. The lack of controls around the data meant that the agency was not able to identify areas that required management attention.

Four of the 15 administrator accounts on SLIP belonged to former staff. The agency's policy for the removal of redundant accounts was not being followed. Failure to remove redundant administrator accounts increases the risk of unauthorised access to the database.

We found that the contracted developers had access to the production environment of the application which allows them to make significant unauthorised changes to software programs and computer systems. This increases the risk of unauthorised changes and could compromise the systems security, availability and confidentiality.

## Government Employees Superannuation Board (Capital system)

The Capital system gets data from a range of sources. Data input and processing is complex and not all automated. The system requires some manual processing and checking of information. This results in a number of 'workarounds' to ensure that the jobs are run in the right sequence, completed successfully and do not impact the business operations. The amount of manual intervention and lack of automated systems also leaves the application vulnerable to human errors and can affect the timely processing of the information.

We found some employees had inappropriate levels of access to transaction files meaning that they could potentially change superannuation accounts and contributions. It would also be unlikely that the agency would detect any changes given the vast number of transactions the system handles.

The application had a number of user accounts with unnecessarily high privileges and no logging of access for any of these accounts, so management would not know whether these accounts were accessed inappropriately. The user accounts gave access to:

- personal information including tax file numbers and addresses
- account details such as user names and passwords
- restricted information about high profile members

We also found six users with 'System Manager' level of access. Two of these accounts were unauthorised. The 'System Manager' group within Capital is the highest privilege level, giving access to all functions within the system. Four of these accounts are not assigned to any individual and it would be difficult to enforce accountability should these accounts be misused.

## Department of Fisheries (FLAMS – Fishing Licensing and Management System)

User access controls for FLAMS were weak. Specifically we found:

- changes made using highly privileged accounts within FLAMS would not be detected
- weak password controls that could be easily guessed
- Fisheries have not defined what access privileges are required by different staff. As a result, inappropriate levels of access had been assigned to numerous users.
- a large number of unauthorised FLAMS accounts. Fisheries did not have a process in place to regularly review user access rights to this system.
- an excessive number of employees were provided with administrator access to the application
- ineffective procedures regarding the monitoring and review of security logs and audit trails within the FLAMS system. There is no logging of changes made directly to FLAMS database records.

We also found that the release and change management processes are inadequately defined and documented. Lack of documentation and high reliance on individuals may negatively impact application support services if any of these individuals leave. In addition the current practices make it difficult to troubleshoot and trace back changes made to the application.

Fisheries' Disaster Recovery Plan (DRP) for FLAMS has not been tested and the Agency does not carry out any formal tests on their backup media to ensure that data or the system can be recovered within a timely manner. As a result, the agency could not be confident that in the event of a disaster it could restore critical information assets.

Fisheries were unable to provide any documentation to demonstrate they were reconciling the number of licence cards sent to the public against invoices for those cards. Fisheries use a third party to send licence cards directly to the public upon payment of fees. They then send a corresponding invoice to the agency for this service.

## Police (SAP – Enterprise Resource Planning System ERP)

Good controls were in place for the SAP systems and we did not report any issues.

# Agency Response

## Department of Fisheries

The Department of Fisheries has commenced a project that will replace the legacy licensing system FLAMS with a modern licensing system incorporating improved controls and functionality. The system is expected to be in use in late 2012. In the interim work is continuing to address issues identified from the review.

## Department of Treasury and Finance (Office of Shared Services – eBusiness)

The Department of Treasury and Finance acknowledges the findings of the Applications Controls Review. These will be finalised by December 2011.

## Government Employees Superannuation Board (Capital system)

At the time of the review additional controls were in the process of being implemented. These controls have now been implemented and include real time notifications that link actions back to a single user. Reviews of user access are conducted regularly to ensure appropriate role based access and the employees identified with additional levels of access are required to carry out business functions.

## Landgate (SLIP – Shared Land Information Portal)

Landgate will utilise the findings of the audit as a key driver for our continuous improvement of the SLIP environment.

## GENERAL COMPUTER CONTROLS AND CAPABILITY ASSESSMENTS FOR AGENCIES

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 2010 we focused on the following control categories:

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

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. We use the results of our GCC work to inform our capability assessments of agencies.

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 work and did capability assessments at 46 agencies. Ten of the agencies were assessed for the first time.

We provided the selected agencies with capability assessment forms and asked them to complete the forms. We confirm and validate agency assessments based on the results of our GCC audits.

We use the 0-5 scale rating[1] shown in Table 1 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.

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.

| | |
|---|---|
| **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. |

**Table 1: Rating criteria**

## What Did We Find?

There was no overall improvement in the capability assessments of agencies when compared to last year.

This year, 64 per cent of agencies fell below the benchmark level for management of IT risks, information security and business continuity.

Figure 4 represents the results of the capability assessments for the 46 agencies. We expect all agencies across the categories should be at least within the level three band.

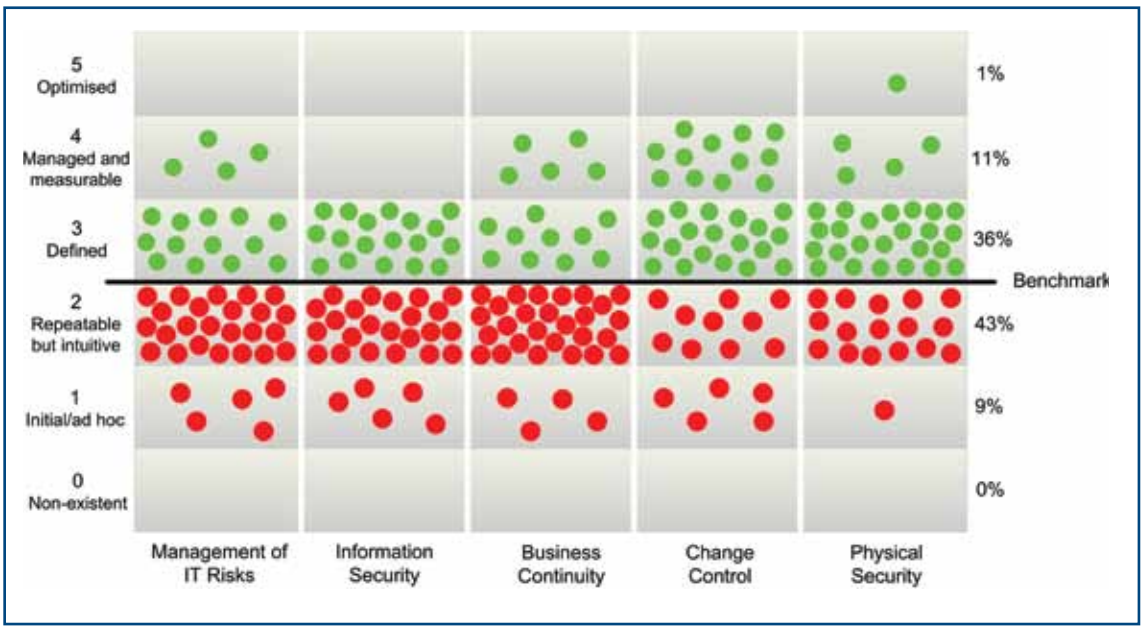



**Figure 4: Capability Maturity Model Assessment Results**

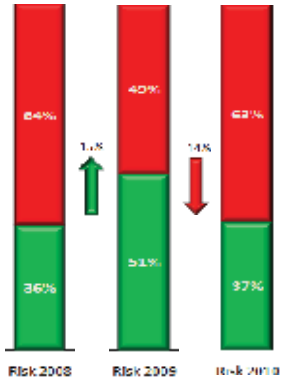
*The model shows that the categories with the greatest weakness were Management of IT risks, Information Security and Business Continuity.*

Trends amongst the agencies that we reviewed last year were:

- 15 per cent improved in at least one category without regressing in any other category
- 15 per cent regressed in at least one category and made no improvement in any other
- six per cent moved up in one category but went down in another
- 43 per cent of agencies showed no change
- 21 per cent of agencies were assessed for the first time.

The following section highlights trends over the last three years for each of the GCC categories examined.

## Management of IT risks



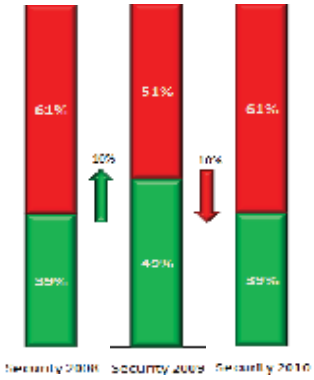

Sixty-three per cent of agencies did not meet our expectations for managing IT risks, a 14 per cent increase from last year. Thirty-two per cent of risk management issues were unresolved issues from the previous year.

Examples of findings:

- A failure at one agency to implement appropriate software licensing controls resulted in the agency using unlicensed software and to an out of court settlement of over $6 million.
- Several agencies either had no risk management policies and practices established or their policies and practices were inadequate.
- Many agencies do not maintain risk registers and lack processes for identifying and communicating risks, even when agency policy requires it.

All the agencies are required by government to have risk management policies and practices that identify, assess and treat risks including IT risks that might affect key business objectives. Failure to properly identify and treat IT risks within reasonable timeframes increases the likelihood that agency objectives will not be met.

## Information security




Sixty-one per cent of agencies were below our benchmark for managing information security, a decrease of 10 per cent from last year. It is clear from the security weaknesses we identified that many agencies have not implemented fundamental controls to secure their systems and information. Thirty-five per cent of the issues were carried over from the previous year.

Examples of findings:

- In several agencies, critical files for payments to staff and external suppliers can be read and manipulated prior to processing.
- Former employees at two agencies had accessed networks and computer systems. Over 2 000 network accounts for former employees remain active across the 46 agencies.
- Users with excessive (million dollar) approval limits, some of whom have the capacity to raise purchase orders, approve the purchase and receipt the goods in the system.

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.

The information security controls we reviewed for our GCC audits are divided into five main areas. The breakdown of findings across the five areas is shown in Figure 5 for all 46 agencies audited.

Figure 5 shows that weaknesses in access controls made up 28 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 25 per cent of our findings. Such weaknesses can leave information and systems on an agency's network vulnerable.

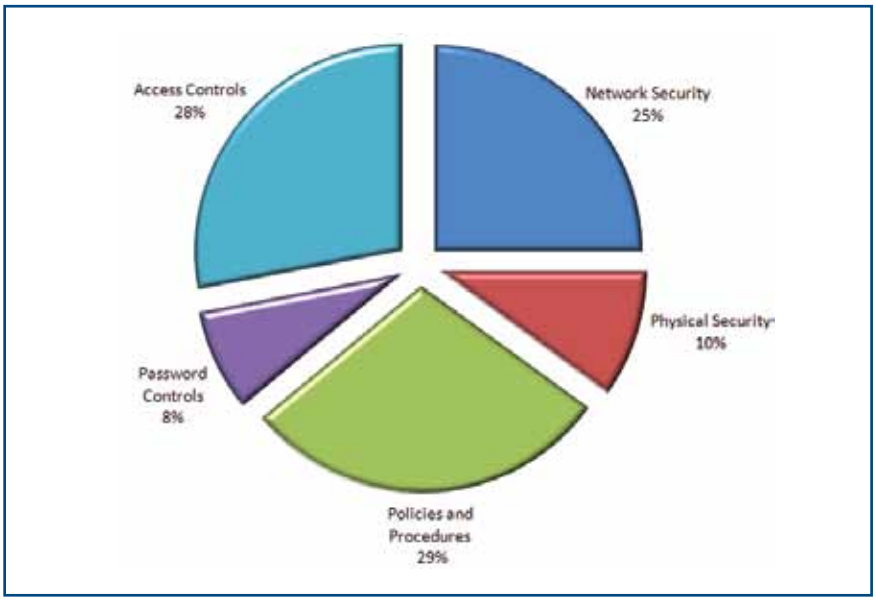
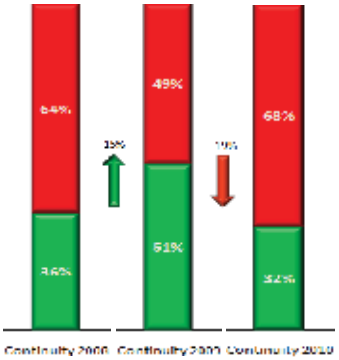



**Figure 5: Security Control Findings**

*The graph shows that access controls and network security were the two most common types of security weakness amongst the 46 agencies.*

## Business continuity




To help ensure business continuity, agencies should have and periodically test their business continuity plan (BCP), a disaster recovery plan (DRP) and an incident response plan (IRP).

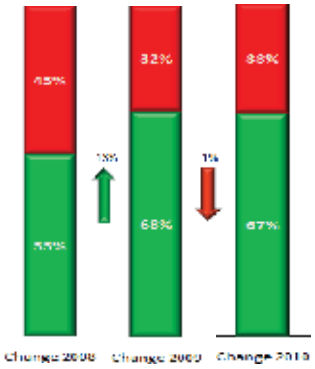
The BCP defines and prioritises business critical operations and determines the resourcing and focus areas of the DRP. The IRP needs to consider potential incidents and detail the immediate steps to ensure timely, appropriate and effective response. Periodic testing is vital for ensuring the rapid recovery of computer systems in the event of an unplanned disruption.

We examined whether plans have been developed and tested. We found a 19 per cent decrease in agencies that meet our benchmark from last year. More than 68 per cent of the agencies did not have adequate business continuity arrangements and 41 per cent of these issues were outstanding from the previous year.

Examples of findings:

- Agencies with no risk assessments or business impact analysis to assist development of BCPs. Some agencies with no disaster recovery, business continuity or incident response plans.
- Some DRPs did not support agency needs as they were developed without any business input.
- Many agencies have not adequately tested and maintained BCPs and DRPs for the recovery of critical systems.

## Change control




We examined whether application 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.

Nearly 70 per cent of agencies were meeting our benchmark for change controls – a marginal decrease of one per cent from last year. We found issues at over 40 per cent of agencies we reviewed. Fifty per cent of these issues were carried over from the previous year.

Examples of findings:

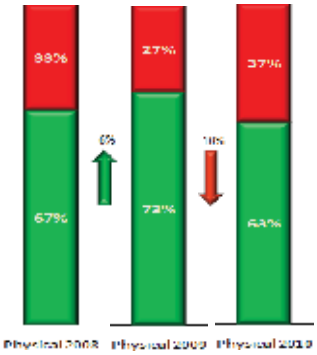
- Agencies with no documented or formal change management authorisation or processes in place for networks, applications or databases, even when their policy requires it.

- Some agencies were unaware of their network configurations and architecture as a result of unapproved or undocumented changes. There was no up-to-date record of current configurations needed to restore or fix critical systems if required.

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. 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



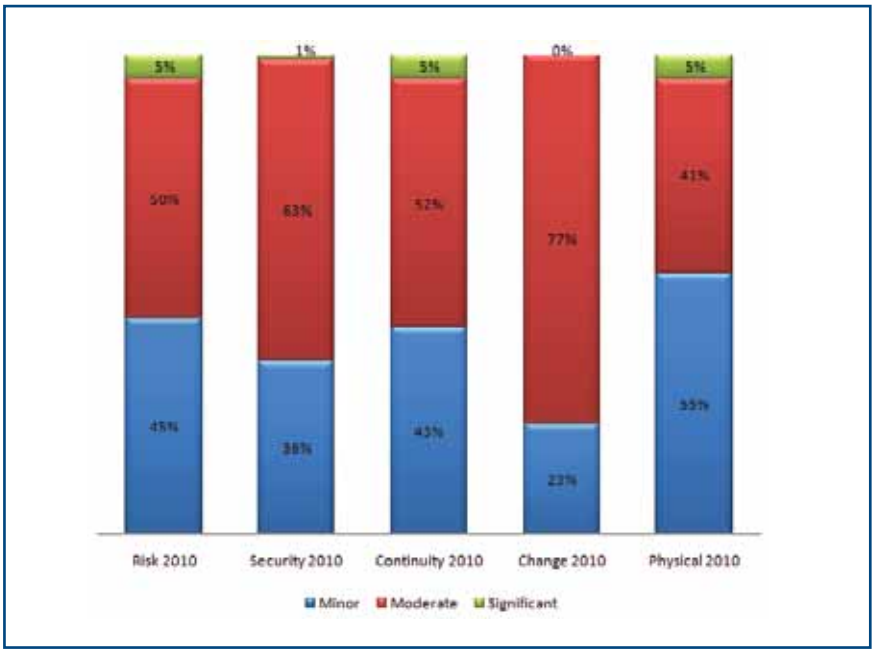

We examined whether computer systems were protected against environmental hazards and related damage. We also determined whether physical access restrictions are implemented and administered to ensure that only authorised individuals have the ability to access or use computer systems.

Sixty-three per cent of agencies meet our benchmark, a 10 per cent decrease on last year. Forty-one per cent of agencies had physical security issues of which 14 per cent were carried over from the previous year.

Examples of findings:

- Many instances of staff, contractors and maintenance people with unauthorised access to server rooms.
- Server rooms lacking environmental controls such as temperature, humidity and smoke alarms, air conditioning and fire extinguishers. Several server rooms were operating at very high temperatures.

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 shows the seriousness of the weaknesses we found in each area we reviewed. 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. A significant finding warrants immediate action, while a minor rating does not pose an immediate threat but still warrants action. However it should be noted that combinations of minor and moderate issues can still leave agencies with serious exposure to risk.