Western Australian Auditor General's Report

Information Systems Audit Report

Report 10 – June 2012

VISION
of the
Office of the Auditor General

Excellence in auditing for the benefit of Western Australians

MISSION
of the
Office of the Auditor General

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

Office of the Auditor General
Western Australia

7th Floor Albert Facey House
469 Wellington Street, Perth

Mail to:
Perth BC, PO Box 8489
PERTH WA 6849

T: 08 6557 7500

F: 08 6557 7600

E: info@audit.wa.gov.au

W: www.audit.wa.gov.au

National Relay Service TTY: 13 36 77
(to assist persons with hearing and voice impairment)

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

© 2012 Office of the Auditor General Western Australia. All rights reserved. This material may be reproduced in whole or in part provided the source is acknowledged.

ISBN: 978-1-922015-10-5

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Information Systems Audit Report

Report 10
June 2012

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
28 June 2012

Contents

Auditor General's Overview

The Information Systems Audit Report is tabled each year by my Office. It summarises the results of the 2011 annual cycle of audits, plus other audit work completed by our Information Systems group since last year's report of June 2011. This year the report contains four items:

- Security of online transactions
- Follow-up audit: Cyber security in government agencies
- Application controls audits
- General computer controls and capability assessments of agencies

The first item deals with how well a selection of nine government agencies were managing the security of their online transactions systems. The payment card industry has a set of required security standards that must be met for anyone that accepts, stores, processes or transmits credit card information. The key focus of the standards is to ensure the security of cardholder data to prevent fraud.

We found that five of the agencies were securely managing cardholder data, while the other four were not meeting all of the required industry security standards. We did not find any evidence of security breaches.

In the second item we followed up our cyber security work from last year by testing a further six agencies. We were pleased to find that the government Internet service provider has implemented controls that blocked most of our attempts to scan and access agency systems. However when this layer of security was removed, we found similar weaknesses in the agencies as last year. We were also able to gain access to agency systems through 'social engineering' attacks that bypassed agency security controls. Agencies need to take a layered or 'defence in depth' approach to cyber security and cannot rely on just one layer of security controls.

In our application controls audits we reviewed a key business application at each of five agencies. The majority of our findings were rated as moderate and minor with over half relating to security control weaknesses. Typical issues included lack of controls over user access and privileges to the applications, and failing to update application software against known vulnerabilities.

Finally our general computer control audits indicate a slight improving trend over the last four years. We use capability maturity models to benchmark agency performance. While the improving trend is encouraging, 42 per cent of agencies are still failing to meet our benchmark in at least one of the general computer control areas we audited.

Security of Online Transactions

Conclusion

Five of the nine agencies we audited were securely managing online transactions. These agencies were not handling cardholder data through their online transactions systems. By choosing not to handle cardholder data, they had substantially minimised risks and compliance costs.

Four agencies were handling cardholder data but did not meet the required industry standards in a number of key areas. These agencies have not effectively managed the risk of cardholder data being compromised.

We found no evidence of cardholder data being compromised. However, we identified opportunities for all agencies to strengthen controls relating to risk management, network security, policies and overall security of their general computer systems.

Background

While the online payment environment has provided government agencies with an opportunity to expand and improve bill payment options, it can also increase the potential for members of the public to be victims of online credit card fraud.

There has been an increasing number of security incidents relating to online systems over the past few years, both internationally and in Australia. On average, online credit card fraud in Australia is estimated to cause $150 million worth of losses each year, with more than 662 000 fraudulent transactions reported.

The Payment Card Industry Data Security Standard (PCI DSS) is a set of standards developed by the PCI Security Standards Council (PCI SSC), a body created by the major payment card brands. The standards focus on protecting cardholder payment and identification information throughout the transaction process. They include requirements for data encryption and ongoing management to ensure security of computer environments that host payment servers and associated applications.

The PCI standard applies to all organisations that accept, process, store or transmit credit card information regardless of size or number of transactions. The level of compliance required varies depending on the number of online transactions, irrespective of the value of the transactions. Any government agency that handles cardholder data in the processing of a payment, should comply with the PCI standard.

Agencies that handle credit card information are required to obtain PCI certification. If an agency is not PCI compliant and cardholder information is compromised, the credit card company can fine the bank up to $100 000 per month for compliance violations. The bank will most likely pass this on to the agency and could cancel the service. Security breaches can also cause loss of customer confidence and reputational damage for an agency.

While compliance with PCI standards is a requirement for agencies handling cardholder data, they should also consider the standards within the broader context of information security.

What did we do?

Our objective was to assess whether agencies have adequate controls to ensure the confidentiality of online payment information, specifically over customer cardholder data.

The key questions we asked were:

- Do agencies have an effective risk management strategy for online transactions?
- Have agencies developed an adequate information security policy that covers security of online transactions?
- Do agencies have effective controls to ensure the network environment is secure to protect online transaction systems?
- Do agencies have effective controls to ensure confidentiality of sensitive information (e.g. cardholder's data)?
- Do agencies have effective controls to monitor network activity and clients' information to protect online systems and cardholder's data?

The nine agencies we selected for the audit were:

- Department of the Attorney General
- Department of Finance
- Department of Housing
- Landgate
- Rottnest Island Authority
- Synergy
- Department of Transport
- University of Western Australia
- Water Corporation

These agencies were selected because they provide online payment facilities to the public.

We assessed the extent to which agencies handled credit card information. This involved reviewing the technical configuration of IT systems including databases, firewalls, network devices and web servers. We interviewed key staff and stakeholders to understand the flow of cardholder data across internal and external networks. Finally, we tested the security of cardholder information throughout the transaction process.

The audit was conducted in accordance with Australian Auditing and Assurance Standards.

What we found

The biggest risk for agencies using online transactions is the security of cardholder data. Cardholder data can include any or all of the following:

- primary account number (PAN)
- cardholder name
- card expiry date
- card verification or security code or value (three or four numbers often required to verify transactions).

Five agencies we audited did not collect or process full cardholder data so were not required to meet PCI standards. Four agencies collected and processed full cardholder data but did not meet PCI standards as required.

We found no evidence of cardholder data being compromised at any of the agencies tested. However, we identified opportunities for all agencies to improve risk management, network security, policies and overall security of their general computer systems.

There were two approaches being used to manage online transactions by the agencies we audited

We found there were two different models used by agencies to manage online payments. All online transactions require a payment gateway or gateway provider. The payment gateway takes cardholder data and transaction details and passes it on to the bank for processing. Typically this is outsourced to a third party payment gateway provider. However one agency had its own payment gateway for passing on cardholder details to the bank.

In the first model, as soon as customers choose to make a payment on the agency website, they are redirected to a payment gateway provider. No cardholder data passes through the agency website. This model carries the least risk for agencies managing online transactions as they do not collect cardholder data during the transaction.

In the second model, when a customer chooses to make a payment on the agency website, their cardholder and payment data is stored and processed through a server owned by the agency before it is passed to the payment gateway. The agency server may be hosted by a third party in a data centre outside the agency network. However the agency is still responsible for ensuring the security of cardholder data. In these circumstances the standards require an agency to obtain assurance that all relevant PCI requirements are met.

Figure 1 below demonstrates the steps for processing an online payment without the agency handling cardholder data (Model 1).

Step 1 The customer chooses to pay for a service or product at an agency web site and is redirected to the Payment Gateway Providers' web site.

Step 2 The customer enters and submits the payment details.

Step 3 The bank processes the transaction.

Step 4 Response from bank through the Gateway accepting or declining the transaction.

Step 5 The customer is redirected to the agency web site to end the process.

Figure 1: Model 1 – Agency management of online transactions

Figure 2 below demonstrates the steps for processing an online payment with the agency collecting cardholder data (Model 2).

Step 1 The customer chooses to pay for a service or product at an agency web site.

Step 2 The customer enters and submits the payment details.

Step 3 The agency payment server passes the cardholder data to the Payment Gateway to transfer cardholder data to the bank.

Step 4 The bank processes the transaction.

Step 5 Response from bank through the Gateway accepting or declining the transaction.

Step 6 The agency Payment Server receives and displays response from bank.

Step 7 The customer is redirected from the agency payment server to the agency main web site to end the process.

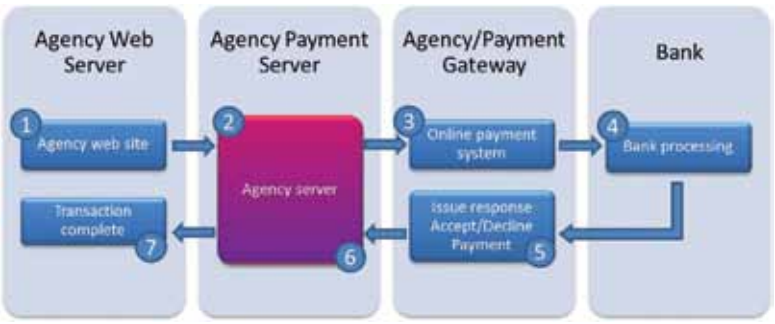


Figure 2: Model 2 – Agency management of online transactions

Five of the agencies used the first model and four used the second model. All of the agencies that used Model 2 were required to be PCI compliant because they either directly handled or were responsible for the handling of cardholder data:

- one hosted the payment server and gateway within their internal network
- one used a third party contractor to host the server and application that managed their online transactions. The server is hosted in a data centre outside the agency network but the agency had not gained assurance that the contractor was PCI compliant
- the remaining agencies hosted only the payment server within their network.

All of these agencies recognised they needed to be PCI compliant, and were taking steps to achieve this, but at the time of our audit they were not PCI certified. Basic requirements of the standards include but are not limited to:

- completing a PCI Self Assessment Questionnaire
- performing quarterly security scans of networks
- completing an Attestation Form required by the standards
- operating a PCI certified payment server
- logging and management review of access to the payment server and database
- gaining assurance that third party contractors are PCI compliant.

Agencies need a structured approach to recognise and manage risks associated with online transactions

While four of the nine agencies we audited stored cardholder data, all agencies that have online transactions systems need to take a structured approach to assessing and minimising the associated risks.

In order to have a secure online transaction environment, agencies must have in place and work through five key processes. These processes are derived from both PCI and information security standards. Figure 3 below illustrates the hierarchy of processes.

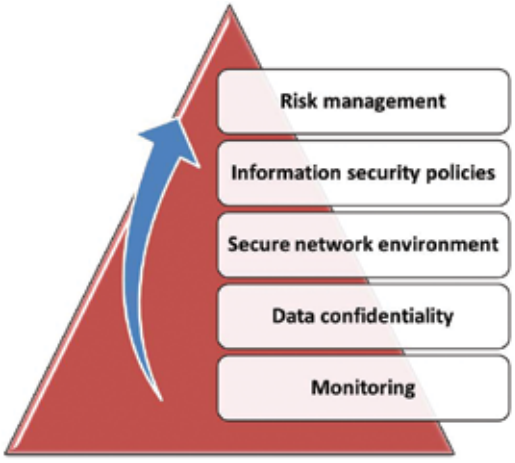


Figure 3: Key process for secure management of online transaction

We assessed each of the agencies against this broader general computer control framework, with a specific focus on security of online payment systems.

Four agencies had either not carried out or not documented assessments to determine the risks associated with having an online payment system. By electing to have an online payment system, the agencies are automatically exposed to the risk of cardholder data being compromised. Their risk assessments should explicitly address this and other risks, and document how these are to be addressed. The choice of model for processing online transactions is a good example of how an agency can significantly reduce risks. If an agency chooses to manage cardholder data through its own server, then it must address the added risks of that approach by ensuring its computing environment, or the environment of a site hosted by a third party, meets required security standards.

Five agencies' IT security policies did not consider or address their online payment systems. We expected that security policies would be up to date and include reference to maintaining a secure network, protecting cardholder data, vulnerability management, strong access control measures and monitoring, and testing of network security.

Three agencies did not have an effective process for applying software updates. Regular updates ensure that critical software and security vulnerabilities are identified and addressed. Some relied solely on having antivirus software and a firewall. This is only one layer of security that can be compromised easily if vulnerabilities are not addressed.

Six agencies did not have incident response plans or procedures to respond to loss of cardholder data or inability to use their online payment facilities.

Recommendations

Agencies should:

- identify and manage risks associated with having online payments. Risks need to be managed within an overall risk management framework
- develop and implement information security policies relevant to their online transactions systems and associated risks. Agencies should consider the PCI standards for guidance in this area.
- establish and maintain a process to ensure software updates are evaluated, tested and where appropriate, applied to their computer systems in a timely manner
- ensure they have appropriately developed incident response plan(s) to address risks associated with online payment systems.

Agency responses

Department of Finance

The Department of Finance is pleased to note that it was found to be securely managing on line transactions by way of adopting Model 1 (as described in this report), which minimises risks and compliance costs.

Department of Transport

Implementation of all the recommendations has already commenced and work is at various stages of completion. Recently the PCI-DSS raised the standard substantially. DoT is working with the Payment Card Industry in examining alternatives available and achieving certification. In the interim, gap analysis has been completed and new processes are in place and we are confident that full personal information of customers is not stored by DoT and hence risk reduced substantially.

Landgate

Landgate welcomes and agrees with the findings of the audit. We are already progressing well towards PCI compliance and have developed our Incident Response procedures with scheduled testing. The applications access is accepted as a small risk but improved review and authorisation processes will be implemented.

Department of the Attorney General

The Department of the Attorney General appreciates the opportunity to participate in the Information Systems Audit: Security of Online Transactions. The Department anticipates that implementation of the Recommendations will be completed by the end of July 2012.

Follow-up Audit: Cyber Security in Government Agencies

Conclusion

Overall cyber security for government agencies has improved due to the government's Internet service provider, ServiceNet blocking common attack methods. However, once this layer of security was removed, agencies remained vulnerable. We found many of the same control weaknesses at agencies that we identified in our previous audit. Our 'social engineering' exploits confirmed that agency staff remain the weakest link in cyber security.

Background

Governments around the world recognise that cyber attack poses a significant threat to national security. They also recognise that the cost of cyber theft is significant. The UK Cabinet Office estimated that cyber theft cost the economy more than GBP 27 billion a year, and they rate cyber attack as a 'Tier 1' threat under their National Security Strategy.

Government agencies often hold critical and sensitive information, so have a responsibility to ensure their IT systems are appropriately configured to detect, manage and appropriately respond to cyber attacks.

In 2011, we 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 non-harmful cyber attacks on the 15 agencies via the Internet. We also scattered USB devices across the agencies as a 'social engineering' test of agency staff. The devices contained software that would 'phone home' and send network specific information across the Internet if plugged in and activated.

In 2011, we found that 'None of the agencies we tested had adequate systems or processes in place to detect, manage or appropriately respond to a cyber attack. The inability of the agencies to detect our attacks was a particular concern given that the tools and methods we used in our tests were unsophisticated.'

What did we do?

This year we conducted a similar assessment at a further six agencies. Our expectation was that agencies had learnt the lessons from our previous report, and had addressed the weaknesses we identified. We also expected that given the high profile of cyber attacks that agencies would take a more proactive approach with the protection of their computing infrastructure and information.

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:

- Does the agency have an effective risk management strategy for cyber threats?
- Is there a security policy and/or framework that address cyber threats?
- Are controls in place to effectively prevent, detect and manage cyber threats?
- Can systems be accessed by exploiting easily identified control weaknesses?

The agencies selected for this audit were:

- Central Institute of Technology
- Department for Child Protection
- Department of Finance
- Polytechnic West
- The Department of the Premier and Cabinet
- WA Police Service

These agencies networks are accessible from the Internet or provide key services to the public and handle sensitive information.

We downloaded free tools from the Internet, including web server and security scanners to perform reconnaissance of agency systems and identify vulnerabilities. We also used intelligence tools for the gathering of information from computing infrastructure. Information gathered in this way can be used to identify both systems and individuals and possible ways to exploit them.

The audit tests were not sophisticated and we did not fully explore all identified vulnerabilities.

We tested agency staff awareness of cyber threats using social engineering techniques. USBs with non malicious code were left on agency premises in public areas. We also used an email 'spear phishing' attack at one agency to see if staff would activate a link designed to provide a back door into the agency.

This audit was conducted in accordance with the Australian Auditing and Assurance Standards.

What we found

This year we found that the government Internet service provider (ISP) ServiceNet had improved security controls. This made it difficult for us to easily scan agency networks. While the hardening of security by ServiceNet is a substantial improvement, agencies cannot rely on this protection alone. It is important that they implement their own controls in line with a 'defence in depth' approach.

The 'defence in depth' principle 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 sensitive information. A graphical representation of the principle of 'defence in depth' security is shown in Figure 4. We have also included some of the weaknesses and controls in the diagram.

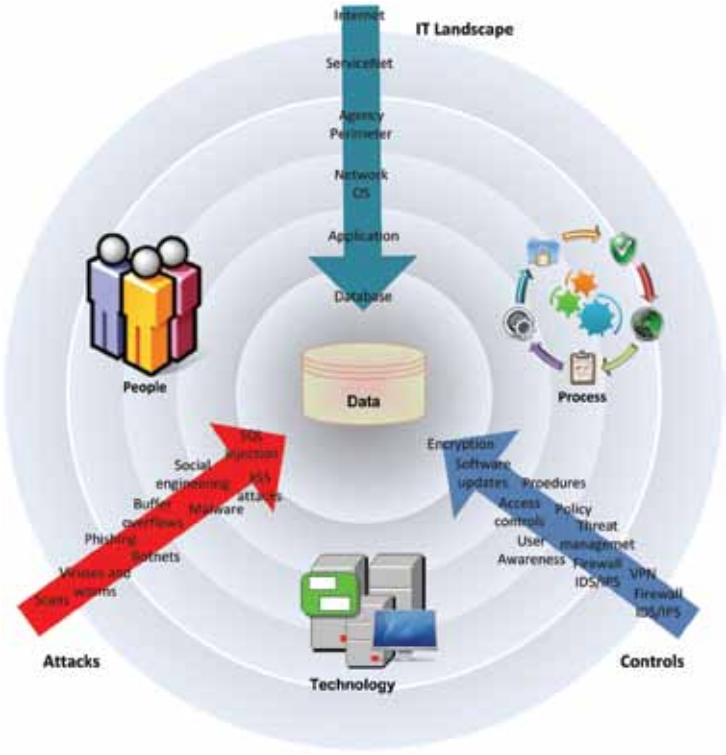


Figure 4 : Representation of the 'defence in-depth' principle

Once ServiceNet allowed our attacks through their firewall, we were able to easily run scans and quickly obtain information regarding agency networks in order to escalate our attacks. None of the agencies we tested had appropriate systems or processes in place to detect or respond to a cyber attack. We exploited a number of the identified vulnerabilities at agencies to confirm the reality of the weaknesses.

Agencies may not have been aware that ServiceNet was providing this first layer of protection against cyber attacks. It is unlikely that ServiceNet would be able to prevent all forms of cyber attack. Agencies have a responsibility to ensure they maintain security over their systems.

Weaknesses identified

In one agency we identified a vulnerability in their online payment system that would allow fraud to be committed. Audit tested this weakness and was able to alter the amount charged for an item and have it delivered. We paid one cent for an item which we later returned to the agency.

In another agency we uploaded non-malicious files to their webserver. Depending on the objective, an attacker could upload files to be viewed by the general public or files with malicious code that could be used to bypass agency security measures without detection.

We identified three significant cross-site scripting (XSS) vulnerabilities on three of the agencies' web servers. An XSS allows an attacker to inject code into a web page which can allow many forms of attack including gaining access and control over systems. An attacker could also obtain sensitive information by redirecting users to bogus sites that appear official.

We were able to identify the web content management systems for each of these agencies which presents an additional vulnerability to XSS attacks. We were also able to establish a connection to escalate our access to these systems.

There were two agencies that were potentially vulnerable to SQL injection attacks. A SQL injection allows the 'injection' of code into a web page in an attempt to execute commands on a database. This means that an attacker can download the contents of a database that the website connects to.

At one agency we obtained personal and sensitive information of 17 employees from scans of webservers. The information we obtained can be used for a number of reasons including social engineering attacks, identity theft or for gaining unauthorised access to systems.

One agency had not applied any software updates to its web server for more than two and a half years. As a result, this particular server had hundreds of vulnerabilities which could have been easily exploited. Some of these could provide system level access to servers, while others allowed the interception of information or could be used as a stepping stone for more sinister attacks. Three other agencies also failed to apply software updates leaving them vulnerable to some exploits.

We found three agencies had poor network infrastructure configurations such as key applications being hosted on the same server. It was also apparent that the routing of internet traffic was poorly implemented. This makes it difficult to identify an attack and understand what occurred.

Why did the weaknesses exist?

From our scans and probes it was clear that the majority of the problems identified were as a result of agencies not applying software updates. We also found many out dated applications and web servers. The combination of these issues makes it easy for an attacker to gather the necessary information to penetrate an agency. In this way, these environments serve as a passage or 'back door' to agency computer systems and information.

None of the agencies had performed risk assessments or developed effective information security policies or incident response plans for dealing with cyber threats and the resulting consequences of an attack. Without consideration of the risks agencies failed to effectively identify controls that would otherwise detect and prevent their computer systems from being compromised. Two agencies did not have any incident response plans while the other four did not have plans that referenced dealing with cyber threats.

The information security policies for the agencies did not specifically consider cyber threats, software updates, loss of information or consider employees and contractors as security threats. Security awareness training had not been performed for agencies to inform them of the risks associated with cyber attacks including social engineering techniques.

Three agencies did not have disaster recovery plans to enable the recovery of systems should an incident adversely affect their systems. Critical systems were not identified and should a cyber attack affect the systems in any way these agencies will not be able to recover in a reasonable time frame.

An important aspect of cyber threats is to recognise reconnaissance work that may be performed by an attacker. Tools freely available from the Internet make it easy for an attacker to identify agency computer networks and gather information to allow calculated and specific attacks against them. Audit downloaded tools and ran them against agency infrastructure to identify the relationships and real links between people, groups of people (social networks), agencies, companies and websites. These scans also returned detailed information regarding internal infrastructure including server names, IP addresses, devices, documents and files including metadata in a simple user friendly format for analysis.

People remain the weakest link

We tested agency staff awareness of cyber threats using social engineering techniques. USBs with non malicious code were left on agency premises in public areas. These USBs were set up to demonstrate capabilities similar to malware that can collect and send information across the Internet or provide ongoing backdoor access to network resources. If activated, the USB sent information back to Audit with basic details identifying the network they were activated from. USBs were activated by several agencies however, these were blocked by ServiceNet. ServiceNet reported traffic from within government networks attempting to establish external connections which were automatically denied. This prevented Audit establishing back door access to those agencies that connected and ran the files on the USB. Some USBs did phone home successfully from private addresses. This test made it clear that employees are still unaware of social engineering techniques which are designed to undermine agency security controls.

As a result of ServiceNet blocking the outgoing traffic initiated by the USBs, Audit attempted an email spear phishing attack on one agency. This is where an email with a link or attachment is sent to an individual to test if they will activate it. Clicking on the link had a similar effect as activating the USB. Within seconds of sending out the email we received an autoreply confirming that the email had passed through protective filtering services and was reaching email in-boxes. The email was only sent to one agency however there were many employees that clicked on the link from different agencies within one day. This indicated that the emails were forwarded on from the original recipient in order to gain from the 'offer' made in the email. Once again, this demonstrated that employees were not familiar with the dangers of clicking on links and in this test we were able to escalate access to those agencies without their knowledge.

Recommendations

ServiceNet can now provide an additional layer of security which supports a defence in depth strategy for improved security. Agencies are encouraged to use, or continue using, ServiceNet for their Internet access and to discuss their security requirements with ServiceNet.

Agencies need to understand the nature of freely available tools and their capabilities in order to understand how an attacker may use them to try to breach security controls and gain unauthorised access to their computer systems.

Agencies can significantly reduce the risks associated with cyber attacks by improving controls through the various layers of security and becoming aware of the threat landscape.

Improvements should be made in the following areas:

- Information security policies, incident response plans, continuity planning, risk management strategies and security awareness training.
- Network design including protective devices and mechanisms.
- Keep operating systems and application software up to date by identifying, analysing and deploying updates as part of a rigorous and formal process.
- Redundant applications should not be accessible from the Internet particularly if they are still connected to internal networks.
- Agencies should make themselves familiar with the Department of Defence top 35 strategies for mitigating cyber threats as well as implement controls that are in accordance with the ISO 27000 security standards.

Agency responses

Department for Child Protection

The Department for Child Protection remains vigilant in protecting information from unauthorised use and will continue to strengthen security controls.

Application Controls Audits

Conclusion

Each of the applications we reviewed had control weaknesses. In total we identified 34 control weaknesses with the five business application systems audited. Security control weaknesses made up 52 per cent of the findings.

The control weaknesses identified have the potential to compromise the integrity, confidentiality and availability of applications and the information they store and handle.

Background

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

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

What did we do?

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

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

- 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.

Figure 5 represents the main elements: people, process, technology and data that are the focus of our application reviews. In consideration of these elements, we follow the data from input, processing, storage to outputs.

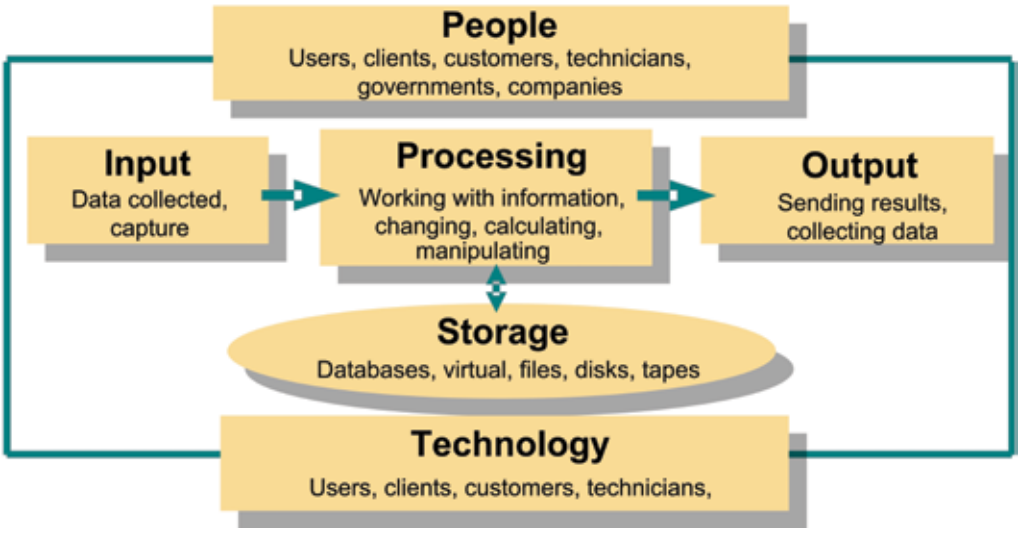


Figure 5: Four areas of our application controls audits

This year we reviewed the following agencies and applications:

- **Department for Child Protection – ASSIST**

  ASSIST is the Department's core client information system, used by field staff and others to record all aspects of case management. It has over 2000 users, and processes about $60 million worth of child and family support payments each year. These include foster care payments, care plan expenses, financial hardship assistance and payments to contractors and consultants providing care services.

- **Mental Health Commission – Psychiatric Services Online Information System (PSOLIS)**

  PSOLIS is used to record and track mental health patient data, including personal details and care provided. The information is used to plan and evaluate services as well as report outcomes to support Commonwealth funding and Key Performance Indicators.

- **Department of Environment and Conservation – Industry Licensing System (ILS)**

  ILS handles around $16 million annually in environmental works approval and environmental licensing fees. Environmental works approval and licensing fees grew by more than 100 per cent over the last four years.

- **WA Health – iPharmacy**

  iPharmacy is the system used for purchasing, dispensing to wards and stock control of pharmaceuticals across WA's public hospitals. WA Health spends over $200 million on pharmaceutical products each year, representing more than a quarter of a million orders from over 250 different suppliers. All of these purchases are managed through iPharmacy.

- **WA Police – Forensic Register**

  The Forensic Register is a crime scene evidence management system. It records every piece of forensic evidence in the State and tracks the transfer of evidence between Police and forensic examination centres.

The audit was conducted in accordance with Australian Auditing and Assurance Standards.

What we found

All of the business applications we reviewed had some control weaknesses. Figure 6 below summarises our findings against each of the agencies applications. Common weaknesses across the agencies included poor access controls. We also found issues with 'other' operational, procedural and process controls that complement effective functioning applications.

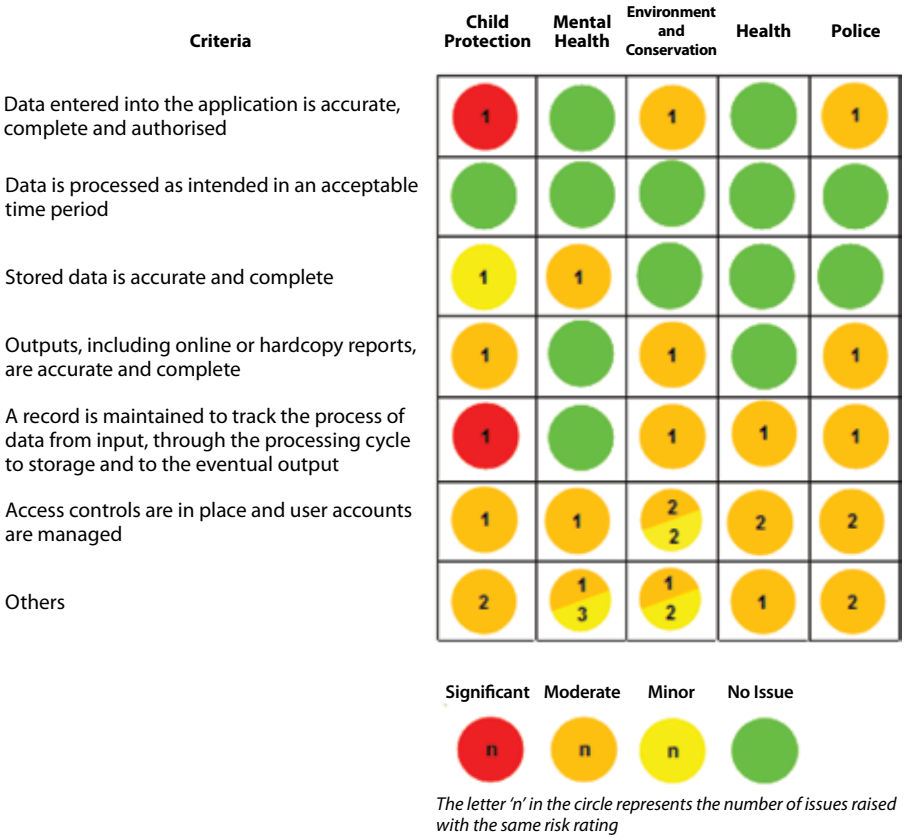


Figure 6: Summary of findings for each business application

We rate our findings as Significant, Moderate or Minor when reporting to agencies. Significant issues are those that present a significant risk to the proper functioning of the application and should be addressed promptly. Moderate issues while not presenting an immediate risk, should be addressed as soon as practicable, while minor issues represent control enhancements that should be considered for future action.

Department for Child Protection – ASSIST

We found that ASSIST has not been configured to prevent staff both issuing and approving payments. For instance, staff who have been given 'Approver' responsibility in ASSIST can approve their own request for payments as well as approving amounts well above their delegated authority. This overrides the basic control of segregation of duties that requires a separate staff member to approve a purchase or payment of another staff member.

There were weaknesses in monitoring and logging of activities within the application. Monitoring and logging is a control used to identify irregular or suspicious activities. Specifically we found:

- no pro-active monitoring of ASSIST application logs to identify any unauthorised actions or suspicious activities
- no audit trail of changes made to ASSIST database records.

There were poor controls over confidentiality and integrity of client information transferred between systems in the agency. Specifically we found the transaction files transmitted from ASSIST to the finance and HR systems are not secured during transmission and the files are stored on network folders that are accessible by all staff. Without restricting access to the transaction files, there is a risk data will be modified, corrupted or deleted.

We found a lack of adequate documentation to support payments made in ASSIST. For example, we noted a $690 reimbursement with 'travel/petrol' as the only explanation of purpose. All government expenditure requires sufficient documentation to justify it is for a proper purpose.

Mental Health Commission – Psychiatric Services Online Information System (PSOLIS)

We found a lack of management review over access to confidential information in the 'cloned' PSOLIS databases that are used for reporting and testing. It is normal practice for agencies to clone their 'production' databases for the purposes of generating management reports that may impact performance of the main database. Clones are also used for testing upgrades to database systems. The same level of management review over who has access to the confidential data in the production database for PSOLIS was not applied to the cloned databases.

Controls over user access to PSOLIS can be improved. We found that user access privileges are not terminated in the application when staff leave employment. Rather access is terminated by removing high level network access to all WA Health systems. As a result, if staff are re-employed in a different area of WA Health, all of their access privileges to PSOLIS are reactivated, even though they may not be required or appropriate.

We noted that the PSOLIS application system is aging, with key components such as the hardware, operating system and database all nearing or past agreed dates for vendor maintenance support. There are no approved plans in place to ensure a smooth upgrade pathway for the application. Future performance of the application may be compromised or more expensive work arounds may be required in the absence of a well thought out upgrade pathway.

Department of Environment and Conservation – Industry Licensing System (ILS)

We found that controls over data input could be improved. Specifically we found that ILS does not logically restrict applicants to filling out only those forms necessary for their requirements. This can result in a waste of time and effort for both applicants and staff processing the applications. In addition the process for recording Geographic Information System (GIS) coordinates is not working properly which can result in incorrect data being entered in the system.

There were a number of weaknesses in the management of user access privileges and review of their activities. These included user names not matching HR staff records; past employees still with access privileges; failure to enforce required segregation of duties; lack of evidence of authorised access to ILS; and lack of monitoring of logs to identify irregular or suspicious activities.

We noted that DEC relies on licensees to estimate discharge quantities each year and license fees are based on this amount. However DEC has no mechanism in place to recover differences if licensees discharge more than their estimates. This also impacts on the accuracy of DEC reporting of emissions by licensees.

WA Health – iPharmacy

We found insufficient logging of user activities and no review process to identify irregular or suspicious activities. There is no review to validate user access privileges or to ensure access to the application functions are within staff delegated responsibilities.

There was lack of documentation confirming staff have received appropriate training before using important application functions such as authorising or ordering pharmaceuticals. In addition there are no scheduled refresher courses to ensure appropriate and consistent use of iPharmacy. Training is important to ensure users are aware of and complying with departmental purchasing requirements for pharmaceuticals.

There were no controls to enforce strong password access for users. Strong passwords help to minimise the risk of unauthorised access to this important application.

WA Police – Forensic Register

We found room for improvement in the way exhibits are logged into and out of the Forensic Register. When an exhibit is sent off-site it is logged out and recorded as been sent to the relevant forensic laboratory. On receipt the laboratory should log the receipt of the exhibit back into the register. We noted a number of cases where through human error, exhibits were not logged as being received. The Forensic Register does not flag delays in the receipt of items. If delays in receipt of items were flagged, this would provide an early warning to both WA Police and the laboratory. Failure to log receipt of items can call into question the integrity of the exhibit if there are periods where location of the item is uncertain.

There were good controls to ensure logging and monitoring of access to the Forensic Register and changes to records. However we consider these could be further strengthened to flag unusual levels of user activity in accessing the register.

We noted that the Forensic Register has not been updated with recommended vendor security patches and configuration updates. We also found that disaster recovery arrangements could be improved to ensure immediate access to a back-up system. Current recovery arrangements mean the Register could not continue to operate seamlessly if there was any disruption to normal functioning of the system.

Recommendations

Reviews of user accounts and privileges should be performed on a regular basis to ensure that access is appropriate at all times. Agencies also need to ensure that appropriate segregation of duties are in place.

Agencies need to log and monitor user activity for their applications. This allows them to identify unusual activities and respond accordingly. This can also serve as a deterrent control against inappropriate access or data theft.

Vulnerability assessments of computing environments and applications should be performed on a regular basis to protect systems from a variety of cyber threats, viruses and malware. Agencies should also ensure that their hardware and software is maintained to ensure support from vendors is available and that the systems can be recovered in the event of a serious disruption.

Agency responses

Department for Child Protection

The Department's new case management system, only implemented in 2010, continues to be enhanced to improve overall internal controls. Significant modifications have been made since the OAG review to address concerns relating to the segregation of duties, audit trails and file transfer security.

Department of Environment and Conservation

DEC agrees with the ten recommendations made by OAG in its management letter to the Department. Action has been completed on five of these; action will be completed on two more by July 2012 and on a further two by quarter three 2012-13. Action on the remaining recommendation relating to online payments has commenced but a completion date has not been set.

General Computer Controls and Capability Assessments for Agencies

Conclusion

We reported 345 general computer controls issues to agencies in 2011. More than half of the agencies we assessed using capability models had not established adequate controls to manage IT Operations, information security and business continuity. Forty-eight per cent did not have adequate controls in place for management of IT risks.

We noted that 54 per cent of agencies we audited this year improved controls compared to the previous year where only 15 per cent made improvements. These were mainly in the areas of change management and physical security. Some agencies have recognised opportunities to implement simple yet effective controls for their environments.

Twenty per cent of agencies had not made improvements in their control environments from the previous year. Eighty-three per cent of these agencies need to make improvements in at least one or more of the audit areas we review each year.

Background

The objective of our general computer controls (GCC) audits is to determine whether the computer controls effectively support the confidentiality, integrity, and availability of information systems. General computer controls include controls over the information technology (IT) environment, computer operations, access to programs and data, program development and program changes. In 2011 we focused on the following control categories:

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

We use the results of our GCC work to inform our capability assessments of agencies. Capability maturity models are a way of assessing how well developed and capable the established IT controls are and how well developed or capable they should be. The models provide a benchmark for agency performance and a means for comparing results from year to year.

The models we developed use accepted industry good practice as the basis for assessment. Our assessment of the appropriate maturity level for an agency's general computer controls is influenced by various factors. These include: the business objectives of the agency; the level of dependence on IT; the technological sophistication of their computer systems; and the value of information managed by the agency.

What did we do?

We conducted GCC audits at 51 agencies and did capability assessments at 42. This is the fourth year we have been assessing agencies against globally recognised good practice.

We provided the 42 selected agencies with capability assessment forms and asked them to complete and return the forms at the end of the audit. We then met with each of the agencies to compare their assessment and that of ours which was based on the results of our GCC audits. The agreed results are reported below.

We use a 0-5 scale rating[1] listed below to evaluate each agency's capability and maturity levels in each of the GCC audit focus areas. The models provide a baseline for comparing results for these agencies from year to year. Our intention is to increase the number of agencies assessed each year.

0 (non-existent)	Management processes are not applied at all. Complete lack of any recognisable processes.
1 (initial/ad hoc)	Processes are ad hoc and overall approach to management is disorganised.
2 (repeatable but intuitive)	Processes follow a regular pattern where similar procedures are followed by different people with no formal training or standard procedures. Responsibility is left to the individual and errors are highly likely.
3 (defined)	Processes are documented and communicated. Procedures are standardised, documented and communicated through training. Processes are mandated however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.
4 (managed and measurable)	Management monitors and measures compliance with procedures and takes action where appropriate. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.
5 (optimised)	Good practices are followed and automated. Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the agency quick to adapt.

Table 1: (Rating criteria)

What we found

More than half the agencies we assessed using capability maturity models had not established adequate controls to manage their IT operations, information security and business continuity. Forty-eight per cent of agencies had not established effective risk management controls and twenty-four per cent had not established effective controls for change management and physical security. Figure 7 represents the results of the capability assessments for the 42 agencies. We expect all agencies across the categories should be at least within the level three band.

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.

Figure 7: Capability Maturity Model Assessment Results

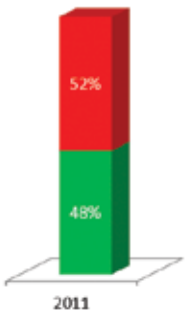
The model shows that the categories with the greatest weakness were Business continuity, IT operations, Information security and Management of IT risks.

In terms of trends, 54 per cent of agencies made improvements in at least one of the categories without regressing in any category which is a significant improvement over last year. Twenty per cent of agencies showed no change compared to last year. Ten per cent moved up in one category but went down in another. Sixteen per cent of agencies regressed in at least one area without making any improvements.

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

IT operations

This is the first year we have assessed IT operations for agencies. Fifty-two per cent of agencies failed to meet our benchmark for performance.



IT operations

The objective for assessing IT operations is to ensure that the service levels provided by IT meet the agencies business requirements. Effective management of IT operations is a key element for maintaining data integrity and ensuring that IT infrastructure can resist and recover from errors and failures.

We assessed whether agencies have adequately defined their requirements for IT service levels and allocated resources according to these requirements. We also tested whether service and support levels within agencies are adequate and meet good practice. Some of the tests include whether:

- policies and plans are implemented and effectively working
- repeatable functions are formally defined, standardised, documented and communicated
- effective preventative and monitoring controls and processes have been implemented to ensure data integrity and segregation of duties.

Examples of findings:

- at two agencies the chief information officers (CIOs) did not manage all aspects of IT resources. This allowed staff to purchase and implement computing infrastructure and software without the CIO's knowledge. These agencies lacked consistent control over their computing environments resulting in poor security and change control practices
- a number of agencies did not have a Service Level Agreement (SLA) with vendors to ensure that service levels are appropriately defined and provided. These agencies were unaware if vendors were fulfilling their obligations and vendors did not report on key activities they were performing. We found that key functions such as maintaining network security, preventing unauthorised access and the monitoring and reporting of security events were inadequate or did not exist
- some agencies have not implemented controls within applications to prevent staff from performing functions outside their normal authority. Staff from one agency were allocated all privileges required to initiate and complete the purchasing of goods with no purchasing limits set. In another agency, a staff member was allocated all privileges required to initiate, change and complete all payroll activities.

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

Management of IT risks

There was a 15 per cent improvement (decrease in issues) of risk management issues from last year, however 48 per cent of agencies did not meet our expectations for managing IT risks. Thirty-two per cent of risk management issues were from the previous year.

Management of IT risks

Examples of findings:

- some agencies had ineffective or limited risk management processes for identifying, assessing and treating IT and related risks

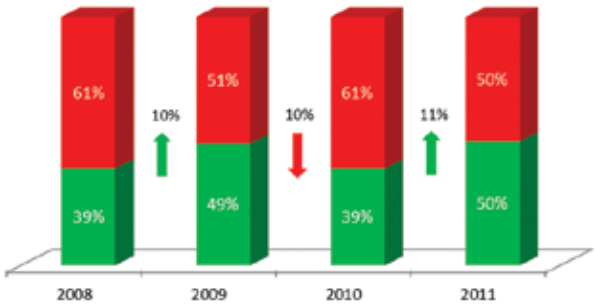
- some agencies have not documented their IT risks in registers for ongoing monitoring and mitigation
- some agencies have not reviewed their IT risks to ensure the relevance of the risks and associated plans. Some were several years old.

All agencies are required to have risk management policies and practices that identify, assess and treat risks that affect key business objectives. IT is one of the key risk areas that should be addressed. We therefore expect agencies to have IT specific risk management policies and practices established such as risk assessments, registers and treatment plans.

Without appropriate IT risk policies and practices, threats may not be identified and treated within reasonable time frames, thereby increasing the likelihood that agency objectives will not be met.

Information security

There was an 11 per cent improvement (decrease in issues) in information security issues from last year. There are still 50 per cent of agencies below our benchmark for effectively managing information security. It is clear from the basic security weaknesses we identified that many agencies have not implemented fundamental security controls to secure their systems and information. Thirty-eight per cent of the issues were carried over from the previous year.



Information security

Examples of findings:

- at one agency we identified 23 user accounts belonging to former staff that were used to log on to the agency's network. One agency had 323 active accounts that were never used
- we found many agencies that had not applied critical software updates to their systems leaving them vulnerable to a variety of cyber threats
- one agency did not require a password for accessing their network. Some agencies allowed weak passwords to be created for key applications and network systems. One agency allowed three character passwords for its computer network.

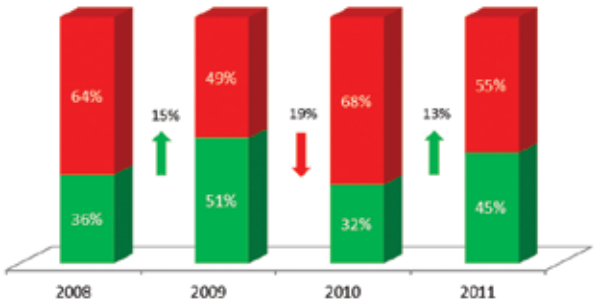
Information security is critical to maintaining data integrity and reliability of key financial and operational systems from accidental or deliberate threats and vulnerabilities. We examined what controls were established and whether they were administered and configured to appropriately restrict access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

Business continuity

To ensure business continuity, agencies should have in place a business continuity plan (BCP), a disaster recovery plan (DRP) and an incident response plan (IRP). The BCP defines and prioritises business critical operations and therefore determines the resourcing and focus areas of the DRP. The IRP needs to consider potential incidents and detail the immediate steps to ensure timely, appropriate and effective response.

These plans should be tested on a periodic basis. Such planning and testing is vital for all agencies as it provides for the rapid recovery of computer systems in the event of an unplanned disruption affecting business operations and services.

We examined whether plans have been developed and tested. We found a 13 per cent improvement (decrease in issues) from last year. Fifty-five per cent of the agencies did not have adequate business continuity arrangements and 38 per cent of these issues were outstanding from the previous year.



Business continuity

Examples of findings:

- some agencies did not have a disaster recovery site or system that would allow them to continue operating in the event of a system failure
- 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
- many agencies have not adequately tested and maintained BCPs, DRPs and backup mechanisms for the recovery of critical systems.

Change control

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

There was a nine per cent improvement (decrease in issues) from last year in change control practices by agencies. Seventy-six per cent of agencies were meeting our benchmark for change controls. We found issues at 24 per cent of agencies we reviewed. Thirty-three per cent of these issues were carried over from the previous year.

Change control

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.

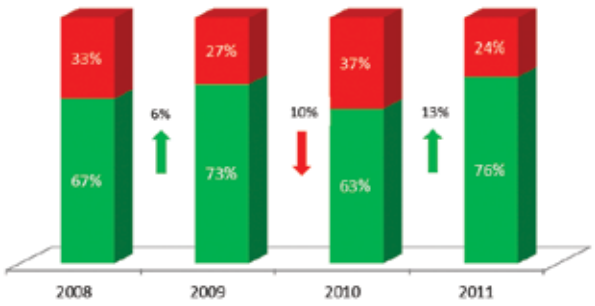
An overarching change control framework is essential to ensure a uniform standard change control process is followed, achieve better performance, reduced time and staff impacts and increase the reliability of changes. When examining change control, we expect defined procedures are used consistently for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

There is a risk that without adequate change control procedures, systems will not process information as intended and agency's operations and services will be disrupted. There is also a greater chance that information will be lost and access given to unauthorised persons.

Physical security

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

We found a 13 per cent improvement (decrease in issues) from last year in agency management of physical security, with 76 per cent of agencies meeting our benchmark. Twenty-four per cent of agencies had physical security issues of which 77 per cent were new findings.



Physical security

Examples of findings:

- some agencies did not have adequate environmental controls to protect their computing infrastructure. One agency had not regularly serviced their air conditioning systems and had inadequate temperature control for the size of room. The room was noticeably warm
- in one agency staff are not available to respond to data centre temperature and humidity alerts after business hours
- in another agency, the fire suppression system for the computer room is a wet pipe system putting people and computer equipment at risk
- some agencies have not appropriately restricted access to their computer rooms. Staff, contractors and maintenance people can access server rooms
- we found some agencies use their server rooms as store rooms for old IT equipment and for general storage.

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

The majority of our findings require prompt action

Figure 8 below provides a summary of the distribution of significance of our findings. It shows that the majority of our findings at agencies are rated as moderate. This means that the finding is of sufficient concern to warrant action being taken by the entity as soon as possible. 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.

The diagram below represents the distribution of ratings for the findings in each area we reviewed.

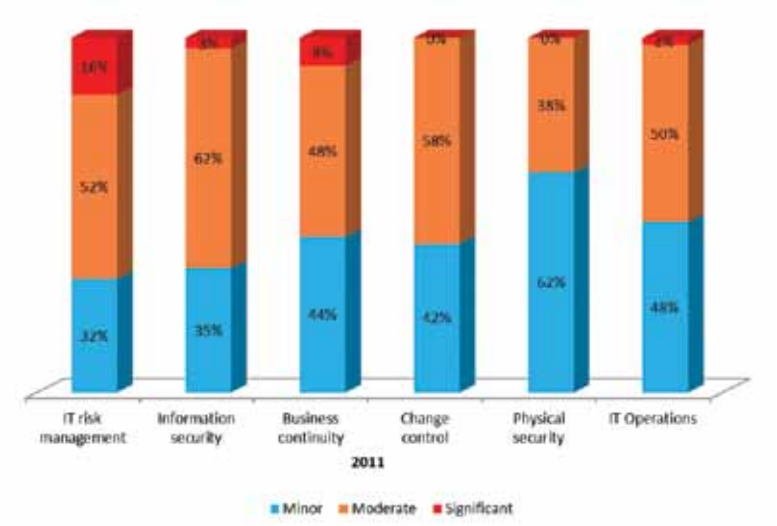


Figure 8: A representation of the distribution of ratings for the findings in each area reviewed

Recommendations

Management of IT operations

Agencies should ensure that they have appropriate policies and procedures in place for key areas such as IT risk management, information security, business continuity and change control. IT Strategic plans and objectives support the business strategies and objectives. We recommend the use of standards and frameworks as references to assist agencies with implementing good practices.

Management of IT risks

Agencies need to ensure that IT risks are identified, assessed and treated within appropriate time frames and that these practices become a core part of business activities.

Information security

Agencies should ensure good security practices are implemented, up to date and regularly tested and enforced for key computer systems. Agencies must conduct ongoing reviews for user access to systems to ensure they are appropriate at all times.

Business continuity

Agencies should have a business continuity plan, a disaster recovery plan and an incident response plan. These plans should be tested on a periodic basis.

Change control

Change control processes should be well developed and consistently followed for changes to computer systems. All changes should be subject to thorough planning and impact assessment to minimise the likelihood of problems. Change control documentation should be current, and approved changes formally tracked.

Physical security

Agencies should develop and implement physical and environmental control mechanisms to prevent unauthorised access or accidental damage to computing infrastructure and systems.

Auditor General's Reports

REPORT NUMBER	2012 REPORTS	DATE TABLED
9	Public Sector Performance Report 2012 – Regional Procurement – Ministerial decision not to provide information to Parliament on the amount of funding tourism WA provided for the Perth International Arts Festival	28 June 2012
8	New Recruits in the Western Australia Police	20 June 2012
7	Pharmaceuticals: Purchase and Management of Pharmaceuticals in Public Hospitals	13 June 2012
6	Victim Support Service: Providing assistance to victims of crime	16 May 2012
5	Audit Results Report – Annual Assurance Audits completed since 31 October 2011 including universities and state training providers and Across Government Benchmarking Audits: Accuracy of Leave Records; Act of Grace and Like Payments; and Supplier Master Files	16 May 2012
4	Supporting Aboriginal Students in Training	2 May 2012
3	Beyond Compliance: Reporting and managing KPIs in the public sector	19 April 2012
2	Opinion on Ministerial decisions not to provide information to Parliament on the amount of funding Tourism WA provided for some events	22 February 2012
1	Working Together: Management of Partnerships with Volunteers	22 February 2012

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.

Office of the Auditor General
Western Australia

7th Floor Albert Facey House
469 Wellington Street, Perth

Mail to:
Perth BC, PO Box 8489
PERTH WA 6849

T: 08 6557 7500

F: 08 6557 7600

E: info@audit.wa.gov.au

W: www.audit.wa.gov.au