Western Australian Auditor General's Report

Information Systems Audit Report

Report 14: June 2014

VISION
of the
Office of the Auditor General

Excellence in auditing for the benefit of Western Australians

MISSION
of the
Office of the Auditor General

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

Office of the Auditor General
Western Australia

7th Floor Albert Facey House
469 Wellington Street, Perth

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

T: 08 6557 7500

F: 08 6557 7600

E: info@audit.wa.gov.au

W: www.audit.wa.gov.au

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

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

ISBN: 978-1-922015-43-3

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Information Systems Audit Report

Report 14
June 2014

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

INFORMATION SYSTEMS AUDIT REPORT

This report has been prepared for submission to Parliament under the provisions of sections 24 and 25 of the *Auditor General Act 2006*.

The information provided through this approach will, I am sure, assist Parliament in better evaluating agency performance and enhance parliamentary decision-making to the benefit of all Western Australians.

COLIN MURPHY
AUDITOR GENERAL
30 June 2014

Contents

Auditor General's Overview

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

The report summarises the results of the 2013 annual cycle of audits, plus other audit work completed by our Information Systems group since last year's report of June 2013. This year the report contains four items:

- Identity Access Management Project at the Department of Health
- Cloud Computing Management
- Application Controls Audits
- General Computer Controls and Capability Assessments of Agencies

In the first item we report on our audit of the Identity Access Management Project at the Department of Health – an important project with potential to impact the successful opening of the Fiona Stanley Hospital. Concern with the project led the Acting Director General of Health to recommend that I audit it. The reasons why ICT projects often run over time and over budget were evident in this project. This report has lessons for all agencies in planning and managing ICT projects.

The second item reports on how five agencies were managing their cloud computing arrangements. Cloud computing is a new business model for delivering ICT resources, but is not new technology. One of the prominent risks of cloud arrangements is the potential threat to data sovereignty and security. We therefore looked at the extent to which agency data was held offshore and at the controls to protect data sovereignty and security. Of concern was that none of the agencies could demonstrate effective contract management of their cloud based services.

The third item of the report contains the results of our audit of key business applications at three agencies. Most of the applications we reviewed were working effectively. However, all three agencies had challenges dealing with systems that had evolved over time to address business needs. We found data integrity weaknesses and time consuming manual processes that could potentially impact delivery of key services to the public.

The final item presents the results of our general computer controls and capability assessments of agencies. It was pleasing to note an increase from three to eight in the number of agencies assessed as having mature general computer control environments across all six categories of our assessment. However, the number of agencies that failed to meet our expectations in three or more of these categories also increased. Nonetheless, the overall result was a slight improvement over the prior year.

The findings and recommendations from these audits should not just be of interest to Chief Information Officers. Chief Executive Officers and other senior managers also need to fully appreciate the opportunities and threats that are inherent within their IT systems. It is not wise or acceptable to push these issues aside for the sole attention of the IT experts.

Identity Access Management Project

Executive Summary

Overview

The Department of Health (Health) consistently accounts for a major proportion of total government expenditure on Information and Communication Technology (ICT) projects every year. Health Information Network (HIN) is responsible for centralised ICT management in Health. HIN is estimated to have spent around $95 million in the past three years on ICT projects related to the commissioning of the Fiona Stanley Hospital, in addition to $87 million on unrelated ICT projects.

As highlighted in past reports, agencies often have difficulty successfully delivering ICT projects, particularly when they involve significant changes and when multiple stakeholders and suppliers are involved.

The commissioning of the Fiona Stanley Hospital (FSH) is the largest project ever undertaken by Health. A small though important part of the commissioning of FSH has been the Identity Access Management (IAM) project which is one of a number of concurrent and interrelated projects planned to deliver a near paperless environment at the hospital.

The IAM was intended to provide users with:

- anywhere, anytime access to the IT systems that the individual is authorised to use
- admittance to those hospital buildings that the individual is authorised to access.

The first phase of the project commenced in 2011. This involved defining all the roles at the Fiona Stanley Hospital that interact with an ICT system, including where people would have to access a building. The clinical and administrative roles would be defined by Health and the support roles by the provider of support services to the hospital.

Health stopped development on the IAM project in October 2013 as they could not see any deliverables from the project. At the time of the decision some $6 million of the $9.2 million project budget had been spent.

In late 2013 the Acting Director General of Health informed us of the difficulties Health was experiencing with the IAM project and requested an audit. Given its potential to impact on the successful opening of Fiona Stanley Hospital, we agreed to assess whether there was adequate scoping, governance and support given to the project.

Conclusion

The IAM project will not be complete when Fiona Stanley Hospital opens later this year. Granting of access to the key IT applications and physical access to the hospital buildings will not be automated.

The reasons commonly found for why ICT projects run significantly over budget and over time were evident in the Identity Access Management Project. Project planning was deficient and governance and oversight including monitoring of progress was inadequate. The business mapping of staff roles to their required ICT access lagged behind the technical development of the solution. Critical technical dependencies and difficulties that threatened the feasibility of the project were therefore not identified in a timely manner. This issue, although raised in successive project status reports, was not elevated to the appropriate levels of management to be actioned.

Key Findings

- Health did not prepare a business case to support their decision to invest funds in the IAM project when it started in 2008. Therefore, they were unable to demonstrate that an informed decision had been made which fully considered alternative options along with system costs, risks and benefits.
- A project initiation document produced in 2012 to re-focus the project deliverables was not supported or approved by the project executive sponsor. This indicated a lack of project ownership and engagement from a critical stakeholder, and increased the risk that the project would fail to deliver its intended objectives.
- Health's tendering process was protracted and arguably did not comply with the State Supply Commission's value for money principle:
    - it took two years to design and issue the tender and then a further nine months to evaluate and award the tender. Protracted processes run the risk of a change in business need and that the tender no longer presents the best business solution.
    - the tender assessment process was based on an assessment of hardware and proprietary software costs for a period of five years. This was despite the IAM being regarded as a long term system. The cost of additional maintenance and other support arrangements were therefore not considered in the awarding of the contract.
    - the successful tender only satisfied 77 per cent of the business and technical requirements. The requirements that were not met were not evaluated for either their criticality to a successful solution or for any cost implications to Health.
- Health did not insist that the successful vendor provide a proof of concept to demonstrate that their system was viable and could deliver the required functionality. Proof of concept provides an invaluable means of demonstrating at an early stage that the proposed system is likely to meet its stated objectives.
- A suitable project governance structure was never established. Though the governance requirements were defined and documented, Health did not implement these. HIN attempted to set up project control groups and business user groups, as per the Health project governance structure at the time. However they were unable to secure appropriate business and stakeholder representation, and these governance mechanisms could not gain sufficient momentum to establish themselves adequately. As a result, there was a lack of project oversight external to HIN and some critical risks and issues from a business perspective were not appropriately escalated and managed.
- Governance, ownership and oversight of the project was undermined by a number of factors including the appointment of the Chief Information Officer (CIO) as project executive sponsor. This meant there was no independent project oversight. In addition, Health delayed engaging a permanent project manager until late 2012, over four years after the project had started and a number of other key positions, including that of CIO and program and project managers were filled by contract staff.
- The monthly reporting for the project was inadequate and did not identify and address key issues in a timely manner. Some of the more important shortcomings were:
    - appropriate project milestones were not used to ensure that the project was on track
    - ongoing difficulties in resolving interdependencies that would impact on project delivery were not adequately highlighted. As a result, they were not escalated for appropriate resolution

- key project risks were not always visible within the monthly report summary. This made it difficult for key stakeholders to manage these risks appropriately.

Recommendations

The Department of Health should:

- enhance its internal capacity to deliver ICT projects.
- for the Identity Access Management project:
  - assess whether the project is able to deliver what it had intended and whether it still matches current need. This will require a focus on user profiling, authentication requirements and rights/privileges management.
- for other ICT projects ensure:
  - the project manager is hands-on at a level appropriate to understand the project issues, particularly where software is developed so that appropriate action can be taken to address risks and issues arising
  - robust business cases exist for all projects
  - project governance structures are put in place and actually operate as intended
  - business project ownership is established early on in a project
  - appropriate involvement of the business in project monitoring and oversight
  - project reporting is effective at identifying and escalating risks to successful project delivery
  - staff in the project team have appropriate and adequate experience with projects of similar scale and complexity. When bringing in external help, the exit strategy should be to up skill internal capacity.

Agency Response

The Department of Health agrees with the findings of the report and supports the recommendations. In this regard, WA Health is currently making a number of changes to improve the governance, management and delivery of ICT projects. This includes the implementation of a new ICT governance structure and the creation of a WA Health ICT Executive Board.

The new governance structure outlines the decision making framework for WA Health's ICT investment. It clarifies the expected roles, responsibilities and accountabilities of all parties involved in the planning and delivery of ICT programs and projects.

This approach will ensure decisions about ICT are business-led and appropriately support the achievement of WA Health's strategic and business objectives. The new arrangements will also ensure rigorous project management and reporting arrangements are in place for all ICT projects. The Executive Board, which is chaired by the Director General and includes Chief Executives of all health services, will be responsible for approving all ICT business cases.

The Department of Health is also making a number of other key changes to support the successful delivery of ICT projects, including:

- the establishment of the role of Chief Procurement Officer in WA Health in January 2014 with oversight for ensuring appropriate policies, procedures, audit and assurance processes are in place across WA Health consistent with legislative and government policy requirements
- progressing other key appointments, including an Executive Director with responsibility for Information and Communication Technology and corporate services and the Chief Information Officer, Health Information Network; and conducting a procurement compliance audit of the Health Information Network; and
- establishing procurement training and education program across WA Health.

With regards to the Identity Access Management project, the Department of Health is currently giving consideration to whether the intended benefits will meet the current or future needs of the health system and appropriate ongoing management of the project.

Background

ICT services are a critical component in the coordination and successful delivery of health and hospital services. They help ensure patient and medical information is accurate and available to the right people when required. An IAM supports the efficiency and security of these ICT services. It provides a single centralised solution for managing users. It also manages their access to information systems and resources appropriate to their role within the hospital.

The IAM project concept came from the 2007 Health ICT strategic framework. This document outlined a vision for the future delivery of statewide computing support to the Health sector. In addition to internal identity and access management, the project was to enable Health to participate in national programs that share and process information with an increasing number of internal and external stakeholders. As increasing numbers of services are made available to a broad range of businesses and individuals, the issue of controlling access to Health's information resources becomes paramount. The proposed delivery of this project was 2017.

The implementation of an IAM solution was a significant investment. The complexities involved made it vital from the outset that the business requirements and risks were fully understood and appropriately documented. This would include a comprehensive business case to ensure that all key stakeholders were fully informed before any commitment was given to the project funding and schedule.

The initial phase of the IAM project had four deliverables with the second, third and fourth deliverables dependent upon the successful completion of the first. The project would:

- identify what access users required to each system, based on their roles in the hospital
- determine how each of the systems grants access to users
- procure and adapt an IAM system
- automate the granting of access, based on the roles identified in the first deliverable. Access would be granted by building connectors between the IAM system and each of the 36 primary systems that people were required to access.

The entire project was given a budget of approximately $7.9 million and a completion date in August 2013. These were later revised to $9.2 million and 23 December 2014 (refer Figure 1).

In September 2010, Health released a Request to Tender for the system. There were seven tender respondents with quotes ranging from $2 599 933 to $17 271 878 and with suitability scores ranging from 58.89 per cent to 77.77 per cent. The successful respondent to the tender had an evaluated price of $4 028 411 and equal highest suitability score.

By the time the project was cancelled in late 2013 it had cost approximately $6 million. Around 25 per cent of these costs were professional services for consultants and contractors. Only one of the 36 connectors between the IAM system and Health's other systems was fully developed at that date.

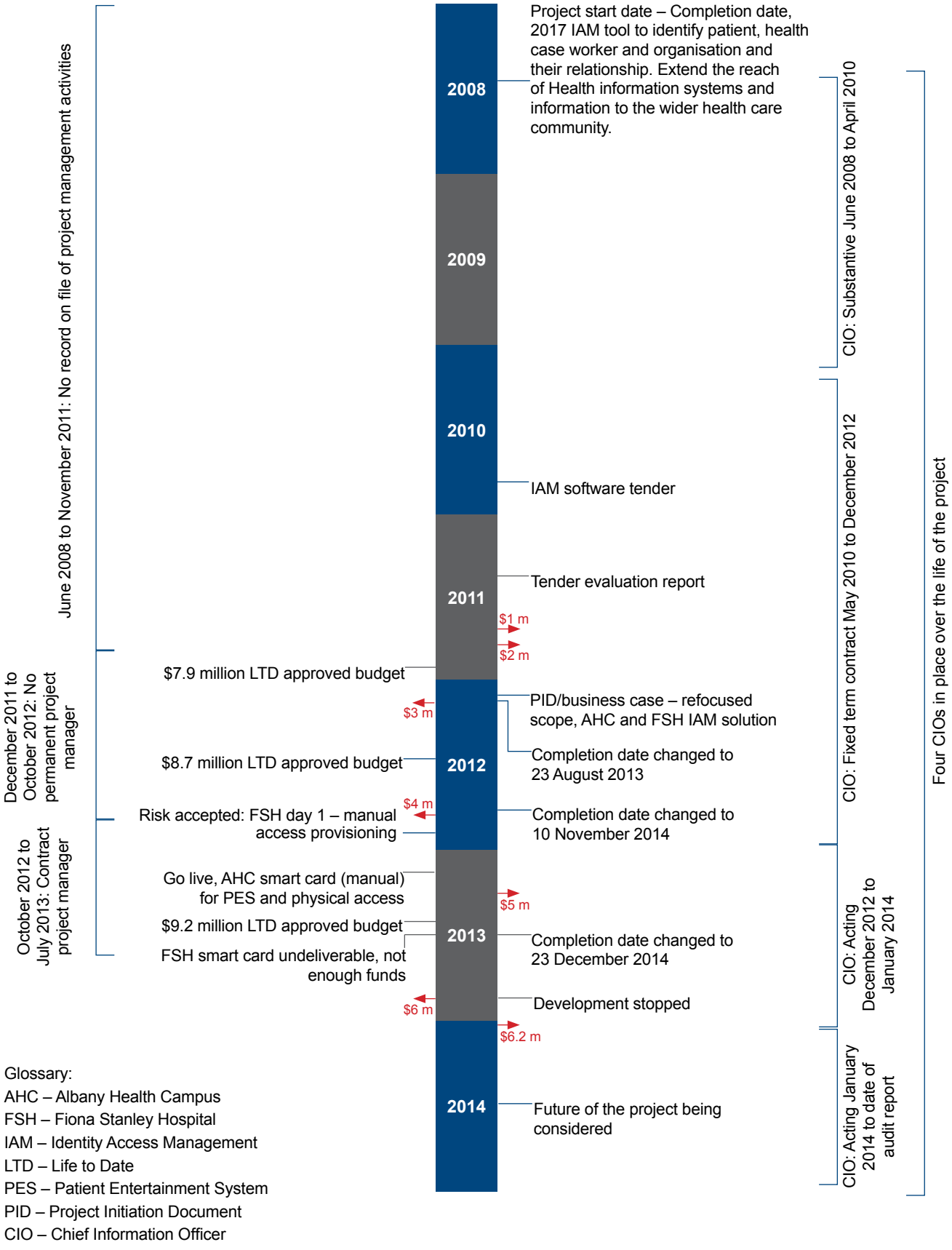

Figure 1: Project timeline summary

What Did We Do?

We liaised with agency and contractor staff to understand the project deliverables and status, and collected and analysed information regarding the project.

To assist our understanding of the project, we developed a project timeline with key milestones and established what was reported to management.

To define what had gone wrong with the IAM project and identify the risks and strategies required to help ensure the project deliverables are achieved in a timely way, we asked the following questions about the project:

- was there adequate scoping?
- was there adequate governance and oversight?
- was adequate support and maintenance in place to implement and sustain the project deliverables?

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

What Did We Find?

The Identity Access Management Project was not adequately planned

In 2008, Health commenced the IAM project without a business case to support this decision or a proof of concept to demonstrate that the proposed system was viable and could deliver the required functionality. The lack of these key planning components was to prove critical in the development and delivery of an effective IAM solution.

A business case is created to help decision-makers ensure that the proposed project will have value and will deliver the required benefits. Thereafter, the business case should be reviewed regularly to ensure that:

- the investment continues to have value, importance and relevance
- the implementation will be properly managed
- the organisation has the capability to deliver the benefits
- the organisation's resources are working on the highest value opportunities
- initiatives with inter-dependencies are undertaken in the optimum sequence.

The result of a review may be to terminate or amend the project. The review may conclude that the business need has changed or the project will not deliver the solution to the business need. The business case is the primary driver for the project so changes to the business case should also mean changes to the project.

One trigger for a review of the business case would be the outcome of proof of concept or a pilot project. A proof of concept was not performed. At the tender evaluation stage the requirement for a proof of concept was replaced by a requirement for a pilot project by the preferred respondent.

However, we were unable to establish if this pilot project and an evaluation of the pilot was completed. Having a successful pilot was essential given the complexity and technical nature of the IAM project, which included old applications with limited ability for adaptation and a large amount of custom and proprietary software to be connected to the IAM software.

Without a properly considered and approved business case and a working pilot or proof of concept, Health could not demonstrate that the intended benefits of the IAM project were clear and measurable or that it had made informed decisions regarding the project.

Scope changes were not properly documented or authorised

In February 2012, the project was refocused from an IAM tool for the business with a deadline of 2017 to an IAM solution for Albany Health Campus and Fiona Stanley Hospital with a deadline of August 2013[1]. This solution would then progressively be applied across the business. A Project Initiation Document (PID), which included a business case, was developed to support this change in the project. However, the project's executive sponsor who was also the CIO did not support or approve the PID.

1 Later in 2012, the completion date was changed to November 2014 and then in 2013 it was changed to December 2014.

We also noted that a range of other scope or budget changes were made without the authority and/or consultation that we expected:

- The physical card access system which was allocated to a contractor was withdrawn by a project manager without consulting the stakeholders. We found no evidence that this change to the scope had appropriate management approval or oversight. There was also no assessment of how this would impact the delivery of the project. The tailoring of the physical card access readers at Fiona Stanley Hospital will now only be completed after the hospital opens.
- Project budgets were amended without proper process or approval. A funding request for the project was lodged on 6 September 2011, but was not initially approved as the requested funds exceeded the available budget. Subsequently on 21 September 2011, a revised funding request was lodged. On 28 September a change request was made that brought the total amount requested up to what was initially sought on 6 September. The change request was to approve the appointment of 3.5 FTE contract staff, including the project manager, at a cost of $801 000 over a period of nine months. This equates to about $1270 per person per day. Although none of the requests were signed the total was reflected in the project budget.

In the absence of properly documented and approved scope changes, Health is unable to determine whether they received value for money and whether the contracted service providers delivered what was intended.

The tender process was deficient

Health took almost three years to award the tender

The Request to Tender (Provision of an Enterprise Identity and Access Management System Inclusive of Installation and Development Services, Training, and Ongoing Maintenance and Support) which includes the main software contract for the IAM project was placed in September 2010. This was more than two years after the project was initiated in June 2008.

Health then took a further nine months, until June 2011, to evaluate and award the tender.

At the point of notifying the successful tenderer, the project had incurred costs of around a million dollars.

We were unable to satisfactorily establish why this process was so protracted. The risk from having such a protracted process, particularly given that there was no review of the business case in that time, is that the tender specifications become outdated and no longer present the best business solution. Also there is an increased risk that the tender submissions will not be relevant and up to date when the tender is eventually awarded.

The total cost was not considered when awarding the tender

Health did not consider the total cost of ownership when it awarded the tender. The tender assessment process was based on an assessment of hardware and proprietary software costs for a period of five years. This was despite the IAM being regarded as a long term system. The cost of additional licencing, software renewal and support arrangements were therefore not considered in the awarding of the contract.

ICT tenders are often awarded on a ‘best fit’ principle rather than the full cost of providing the business requirements. The full cost includes hardware and software for the life cycle of the project, costs associated with proprietary software and costs to address any shortfalls between the business need and the prospective tenderer.

Health selected the supplier based on a tender response that addressed only 77 per cent of their business and technical requirements. They did not determine how critical the shortfalls were to the overall project or identify how and at what cost they should be addressed. Examples of the requirements that were not fully addressed included:

- those that would incur additional licencing costs as the software would have to be duplicated at a number of sites
  - the ability to provide a 'virtual' directory. The tenderer proposed using 'views' instead
  - managing passwords in the event of a network failure
  - caching of entitlement policies
- the need for a test environment
- support for custom approval screens that will survive a product upgrade
- support for certain web and mobile browsers
- a software development kit.

Health's stated vision for the IAM system was that it would be in long term use. Despite this, the price evaluation process only considered software licensing and hardware costs for five years. The cost of additional licencing, software renewal and support arrangements were therefore not considered. We note that the State Supply Commission's 'value for money policy principle' is that the full cost of providing all the technical and business requirements be reflected in decisions to award a contract.

When the full business and technical requirements are not met, there is an increased risk that a project will suffer from limited adoption, require expensive retrofitting or the use of 'workarounds'. All of these may result in unnecessary security risks and substandard business performance.

Health's project governance framework was not followed

Project governance is the framework which ensures project decisions are structured, transparent, authorised and based on accurate reliable information.

Although the project governance requirements were defined and documented in the PID, Health did not implement these. As a result, Health lacked critical oversight to ensure the project was properly designed, planned and managed for the successful delivery of objectives.

The project's executive sponsor was also the CIO

The executive sponsor for the project was also Health's CIO. Good practice is normally to have an executive sponsor who is neither part of the IT group or part of the business area. An executive sponsor who is independent of both the IT and the business area is best able to ensure that the project is aligned with the needs of all stakeholders and to provide objective oversight of the management of the project.

The fact that the executive sponsor was not independent was raised as a high risk in the PID. This risk was only addressed toward the latter part of 2013 when the project was already behind schedule. Addressing risks in a timely manner is key to ensuring successful project delivery.

The project executive sponsor was not properly supported

The PID contained a requirement for a Project Control Group (PCG) to provide critical support to the executive sponsor. However, this important role was never made operational. HIN attempted to set up a project control group but they were unable to get appropriate business and stakeholder representation. This important governance mechanism was therefore not established.

The PCG's role was to advise the executive sponsor and to approve the approach and procedures for project management. As well, they were to approve the criteria to be used for accepting completion of each stage of development and to provide a quality review of each stage. However, even if the PCG had been operational, we note that no success factors were defined for each stage of the project.

The PCG's responsibilities were also to include:

- control over the development of detailed plans, including schedule, milestones and expenditure for the project
- monitoring the management of project risks and ensuring appropriate action is taken to address high risk areas
- monitoring progress of the project against plan, budget and achievement of intended outcomes and benefits, providing support to resolve key issues that arise.

In the absence of the PCG, the executive sponsor relied on the project manager and program manager to provide assurance that the project was on schedule. However, given the roles of these two positions, fully impartial and objective advice could not be assured.

A further factor that weakened the governance of the projects was that the project manager position was not filled for much of the project. This impacted heavily on the day to day management of the project and further compromised the information flow to the executive sponsor.

Monthly project monitoring and reporting was inadequate

The monthly reporting did not enable management to identify and address key issues in a timely manner. For the duration of the project the monthly reporting included the detailed project reports of 29 to as many as 99 projects in one report. This method of reporting is not ideal for managers, making it difficult to identify the key issues and make decisions.

There was no evidence that the project milestones were appropriately monitored by management. The monthly Portfolio Status Reports (PSR) only included milestone reporting until December 2012 and these were not aligned with the project deliverables and key dependencies. These milestones provide a control mechanism for ongoing project oversight and help ensure the project is on track regarding cost, deliverables and time scales.

Ongoing project issues were not escalated. For example, technical difficulties were experienced due to the inability of the existing Health proprietary software and the software of the main hospital support providers to work with the IAM System.

Also, risks that had been accepted at the project level were not always visible at the management level. One example is the acceptance of the risk in November 2012 that the project would not be ready to function at FSH on day one.

The business processes lagged behind the technical development

The need for the business to be suitably engaged in the IAM project was recognised in the PID as an issue of high importance and risk. Despite this, management failed to give the project the attention it required.

The need for greater management attention to the project was evident in a number of ways. For instance, successive monthly PSRs noted that the technical development of the project was being based upon generic business mapping of staff roles. This generic information was used because the actual specifications from FSH, the Albany Health Campus (AHC) and from the private provider of the support services to FSH, had not been supplied. As a result, the technical limitations that impacted on the feasibility of the project were not identified.

The overall consequence of the failure to develop the IAM is that physical admission and access to the key IT applications that would enable FSH to operate in a near paperless environment will not be automated when the hospital opens later this year.

The modules that would allow the IAM system to communicate with the various clinical and human resource applications were also not ready when AHC opened in April 2013. However, card access to the hospital doors, based on user roles, was successfully trialled at AHC. Subsequently, the process reverted to accessing all doors except to the Pharmacy and Records area. This change was necessary because of inaccuracies in the matrix that determined which role should access which parts of AHC.

Cloud Computing Management

Executive Summary

Overview

Cloud Computing can be defined simply as '*an outsourcing arrangement whereby a service provider will host information systems or resources. These systems and resources are then accessed by the client over the Internet (the cloud)*'. Cloud computing is not a new technology but it is a new business model for delivering ICT resources.

Benefits from accessing shared resources over the Internet can include; improved flexibility, increased scalability and greater availability and resilience. Examples of these sorts of benefits include not having to house IT infrastructure on-site and only paying for services used. These benefits can improve cost effectiveness and also potentially reduce ongoing operating costs through the reduction of IT infrastructure and staff.

However there are also risks relating to data security and sovereignty, system performance, unauthorised access, legal and regulatory compliance and loss of access to the system, service or information. These risks will vary depending on the sensitivity of the agency's information and the criticality of the service. Data sovereignty issues arise when data stored 'offshore' in other countries becomes subject to local laws potentially affecting the rights over that information.

More agencies are considering the option of moving some of their information systems to the cloud. In doing so they need to fully understand and consider both the benefits and risks associated with cloud computing before making a decision to adopt.

The objective of this audit was to assess whether a sample of five agencies were effectively managing their cloud computing arrangements. We also examined the extent to which agency data was being held offshore under the cloud arrangement and whether there were appropriate controls to protect data sovereignty and security.

The sampled agencies were the Department of Fisheries, Department of Sport and Recreation, Metropolitan Redevelopment Authority, Public Sector Commission and Public Transport Authority.

Conclusion

None of the five agencies could demonstrate effective management across all of the key areas relating to their implementation of a cloud based service with a consequent risk to the confidentiality, integrity and availability of information. Common weaknesses included not assessing business risks and costs and benefits of shifting to the cloud, inadequate contractual arrangements, and weaknesses in the IT security and business continuity arrangements. Despite these overall failings, some agencies demonstrated elements of good practice across certain key areas in their management over cloud services.

Weaknesses in the contractual arrangements with the cloud service providers included a lack of specificity relating to whether agency data can be stored offshore. Agencies were therefore trusting their service providers not to store their information outside Australia and to not allow access to their information from offshore locations. Currently, the data of only one agency (back-up data) is stored offshore.

We noted that government guidance to WA agencies on offshore storage of information and other issues related to agency decisions to move to the cloud was minimal. However, both the Department of Finance and the State Records Office are producing material that will help close this gap – action that is necessary as the trend towards cloud computing grows.

Key Findings

- **Risk Management** – four of the five agencies were not effectively managing the risks associated with their cloud computing arrangements. In particular, these risks related to information security and sovereignty, system performance, unauthorised access, legal and regulatory compliance and loss of access to the system, service or information. If these risks are not managed properly, they could have a significant impact on an agency's key objectives and operations and result in the loss or disclosure of information. The overall lack of effective risk management was evident across the following key areas:

- **Business Case** – only two of the agencies had a business case to support their decision to implement a cloud based service.

    - **new service –** two of the agencies could not provide adequate documentation to support their recent decision to implement a new cloud based service. These agencies were unable to demonstrate that an informed decision was made to deliver key systems or services using the cloud. They were unable to show they had fully considered and evaluated the service costs along with the risks and benefits.

    - **service renewal** – in those instances where contracted services were up for renewal there was again limited evidence by two agencies to show appropriate consideration was given to alternative options, costs and benefits.

- **Contract Management** – all five agencies had weaknesses in the contractual arrangements established with their service providers. Examples include:

    - **sovereignty** – no contractual requirements or limitations on where agency data could be stored. Agencies were generally unaware of whether their data could be stored offshore under the terms of the agreement. However, given that the agreements were with multi-national companies, there would seem a real possibility of the data ending-up off shore if not explicitly excluded by contract. Currently, the data of only one agency (back-up data) is stored offshore

    - **security** – no contractual requirements relating to data security controls that the service provider should implement to protect the confidentiality, integrity and availability of agency data

    - **service continuity** – no contractual obligations on both parties in the event of a planned or unexpected termination of the services

    - **performance** – no contractual requirement for the service provider to report to the agency on the provider's performance or on any relevant security matters.

    Failings in contractual terms and conditions along with poor contract management and oversight increase the risk that the cloud service will not meet an agency's requirements. This could result in a poorly performing and insecure service or sensitive information being stored offshore.

- **Information Security** – three of the agencies had a range of weaknesses in the information security controls implemented by their cloud service provider. These weaknesses increase the risks to the confidentiality, integrity and availability of agency information and included:

    - known software vulnerabilities that had not been fixed or updated

    - information was not being securely deleted from hard drives before they were reused or destroyed

    - sensitive information on backup tapes was not being encrypted

    - intrusion detection systems (IDS) had not been appropriately deployed. Without an IDS it is less likely that any cyber-attacks will be detected.

- **Business Continuity** – all five agencies had weaknesses in their business continuity and/or disaster recovery plans and arrangements. These arrangements are important because they should ensure the continued operation of the cloud service in the event of an unplanned outage, major incident or a service provider ceasing operations. We identified that agencies and/or the cloud service provider lacked adequate plans to restore services and business operations in a timely manner. Without appropriate and tested plans, services may be interrupted for prolonged periods with a significant impact on the public and agency operations and staff.
- **Guidelines** – agencies should ensure they are familiar with and utilise the Department of Finance resources covering cloud computing arrangements.

Recommendations

- **Risk Management** – agencies engaging a cloud service should ensure it is supported by an appropriate risk management process throughout the service lifecycle. This process should ensure all relevant and emerging threats and vulnerabilities related to an agency's service, information and cloud service provider are identified and assessed. The agency should have appropriate treatment plans in place to address these risks.
- **Business Case** – it is important that agencies properly assess and document their decision to adopt cloud based services. This assessment should ensure any cloud based arrangement is evaluated against other viable options. As a minimum, the evaluation should consider the costs, risks and benefits of each option. As part of this work it is important that agencies implement a process to monitor, evaluate and report against the projected costs, outcomes and benefits.
- **Contract Management** – the contract between the agency and service provider must include appropriate terms and conditions to address and mitigate key areas of risk. Agencies should implement appropriate management and oversight arrangements to ensure the service provider is adhering to the contract. This may involve periodic reporting, regular audits and service provider certification.
- **Information Security** – to adequately protect the confidentiality, integrity and availability of information, agencies must ensure that appropriate security controls are implemented. Service providers will charge a fee for the implementation and management of these controls. Therefore, the type and level of controls used should reflect the value and risks to the agency information. Agencies should implement suitable mechanisms to gain regular assurance that the controls are implemented and working effectively.
- **Business Continuity** – agencies should make sure that their service providers have adequate and tested business continuity and disaster recovery plans in place. Agencies should also develop their own business continuity and disaster recovery plans if their service providers systems are unavailable or the service provider ceases to operate.

Agency Responses

Department of Fisheries

The Department is fully aware of the shortfalls of the current contract and is seeking to resolve these issues. However, it must be noted that at the time that the Department secured this contract there was limited information available to assist agencies in purchasing solutions of this nature. I am confident that the Department took into consideration the information available at the time by seeking advice from officers at the Department of Finance and also by appointing a consultant to manage the tender process and draft the contract. The residing contract and tender process was approved by the Department of Finance, approved by the independent probity Auditor and also by the State Tender Reviews Committee and was passed with no comment at the time.

Department of Sport and Recreation

The Department of Sport and Recreation (DSR) acknowledges the Auditors findings. DSR commenced a HR Business Systems Review in April 2014 to consider the business case for our future HR Information management requirement. Additionally, DSR is committed to reviewing its Business Continuity Plan.

On receiving six weeks notice for the expiry of the Talent2 contract, DSR was engaged in a process for reviewing other business systems. Therefore the agency had limited resources to adequately consider a proper requirement within the available timeframe.

Metropolitan Redevelopment Authority

The Metropolitan Redevelopment Authority will ensure that the concerns raised are addressed and taken into consideration in the further development and review of the crisis management framework components. Interim measures will be considered to ensure that all findings are addressed in the immediate future and internal processes modified to ensure due consideration is given and action taken.

Public Sector Commission

The Public Sector Commission (the Commission) welcomes the review and agrees with the recommendations in the Auditor General's report. Discussions have been held with the provider of the WA Government eRecruitment system and the Commission will act on the recommendations as a matter of priority to further improve the contract and the service provided.

The Commission considers its contract with the provider of the WA Government eRecruitment system to be in the most part robust. The process undertaken for the new contract was complex, detailed and in accordance with the Government procurement guidelines. It resulted in a solution that meets requirements within budget and represents value for money. Due diligence in the areas of contract management and technical security was undertaken in accordance with the established procurement and legal framework. Appropriate expertise was utilised in this process.

However, it is acknowledged that some aspects of the contract, in particular reporting on the depth of IT Security controls in place, should be further improved. The Commission will undertake action to increase the reporting of IT security protocols as per the Auditor General's recommendations. The Commission has a very thorough Service Level Agreement with the provider that is reported on monthly and reviewed at an executive level on a quarterly basis.

The Commission also supports these recommendations being provided to Government Procurement for consideration and will work with them to implement any changes to the procurement process.

Public Transport Authority

Participating in such an audit is constructive for an organisation such as the PTA considering that cloud computing is an increasingly common business practice. The PTA is also pleased in regard to the whole of Government approach to the management of cloud computing from a policy perspective.

The PTA welcomes the point that Government is aiding agencies with strategic direction in relation to cloud computing. With the accelerated growth of the cloud computing it is important that future project managers within the Divisions of the PTA consider the risks associated with the use of the Internet in this way. Having guidance from the Department of Finance and the State Records Office gives management from the PTA confidence that risks will be considered and action plans will be formulated to mitigate the risks. The PTA believes the Department of Finance "Cloud Toolkit" and the "Cloud Planning Flowchart" guidance tools will be invaluable when next preparing Business Cases for future Cloud related projects.

In this regard the PTA Manager Information Services has been requested to prepare a PTA policy and guideline, based on the Department of Finance and the State Records Office guidelines, for consideration and endorsement by PTA's Information and Communications Steering Committee. This policy and guideline will then be applied to all future PTA developments incorporating cloud computing.

Background

There are a number of definitions for cloud computing but for the purpose of this report we are using the following definition: *'Cloud computing is an outsourcing arrangement whereby a service provider will host information systems or resources. These systems and resources are then accessed by the client over the Internet (the cloud)'*.

This arrangement of accessing shared resources can offer a number of benefits which include cost effectiveness, improved flexibility, increased scalability and greater availability and resilience.

Cloud computing is not a new technology but rather a new business model for delivering ICT resources. Because of this, many of the risks and issues associated with ICT service delivery remain. However, as most agency systems were designed to operate in a secure environment, agencies need to fully understand the risks associated with cloud computing both from an end-user and agency perspective.

The risks relate to areas such as data security and sovereignty, system performance, unauthorised access, legal and regulatory compliance and loss of access to the system, service or information. Data sovereignty is important as digital information is subject to the laws of the country where it is located. These risks will vary depending on the sensitivity of the agency's information, the criticality of the service and how the cloud service has been implemented by the service provider.

From our ongoing work we are seeing more government agencies investigating the use of cloud based services and options. Therefore it is vital for government that agencies fully understand and consider both the benefits and risks associated with cloud computing before making a decision to adopt.

There are a number of different models and options for delivering cloud based services. The three most common service models are:

- ***Software as a Service (SaaS) –*** the consumer uses the provider's applications running on a cloud infrastructure to deliver a specific function or service.
- ***Platform as a Service (PaaS) –*** the consumer can install or develop applications onto the provider's cloud infrastructure.
- ***Infrastructure as a Service (IaaS) –*** the consumer is provided with fundamental computing hardware and resources where the consumer is able to install and run operating systems and software applications.

An agency can adopt any combination of the above models and more than one provider can be involved in the delivery of each model. For example an agency's data centre, protective devices, architecture and software could be controlled and maintained by three different service providers.

The WA Government has not as yet provided guidance to assist agencies who wish to adopt cloud services. However, guidance and examples of good practice are available from the Australian Signals Directorate, Australasian Digital Record Keeping Initiative and the Commonwealth Department of Finance and Deregulation.

The WA Department of Finance is preparing to release a set of guides and toolkits to help agencies and inform industry in the transition to a suitable cloud computing solution. The toolkits and the cloud planning flowchart assist agencies to determine their business case including risk, scope, benefits and potential cost to implement the solution. It is essential that this planning is done prior to the procurement phase.

What Did We Do?

Our objective was to assess whether agencies were effectively managing their cloud computing arrangements. We also examined the extent to which agencies had stored data offshore and whether there were appropriate controls to protect data sovereignty and security.

The specific lines of inquiry were:

- did the agencies adequately consider the costs, benefits and risks prior to outsourcing one or more of their key IT systems into the cloud and throughout the lifecycle of the service?
- did the agencies implement appropriate contracting arrangements to effectively manage their cloud computing services?
- have cloud service providers implemented adequate IT controls to satisfy the agreed obligations and agency requirements?
- have the agencies evaluated, monitored and reported the costs and benefits of using the cloud model?

The agencies selected for the audit were:

- Department of Fisheries
- Department of Sport and Recreation
- The Metropolitan Redevelopment Authority
- Public Sector Commission
- Public Transport Authority.

We also consulted with the Department of Finance who previously entered into a common user agreement for a cloud based human resource system for agencies. A large number of agencies use this system.

The State Records Office (SRO) and Information Commissioner both have an interest in how agencies manage their information in a cloud arrangement. The SRO is developing a new guideline to provide information management advice on cloud computing specific to WA government agencies. We invited both to provide their views on cloud computing and these are included in full at Appendix 1.

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

What Did We Find?

A high level summary of findings is shown in Figure 1 below against the key areas we examined. These areas are not exhaustive but are considered important to the management of cloud services. The findings are categorised based on the levels reported to each agency. The table shows that no agency demonstrated good management over cloud services across these areas.

	Agencies Audited				
Audit Area	**Department of Fisheries**	**Department of Sport and Recreation**	**Metropolitan Redevelopment Authority**	**Public Sector Commission**	**Public Transport Authority**
Business Case / Tracking Costs and Benefits (The decision to select a cloud service was based on a full understanding of costs, risks and benefits.)					
Risk Management (Risks throughout the cloud service lifecycle have been adequately identified, assessed and treated.)					
Contract Management (Cloud service contract contains appropriate terms and conditions to meet service requirements. Oversight and management of the contract and service provider is adequate.)					
Information Security Controls (Appropriate and effective security controls are in place to protect the systems and information.)					
Business Continuity / Disaster Recovery Plans (The agency and service provider have adequate and tested plans to maintain the cloud service.)					

Figure 1: High level of summary of findings

Note: For the Metropolitan Redevelopment Authority the issues shown in the table combine the issues from audits of the two cloud services they are using.

	**Significant** finding where there is a significant risk to the entity should the finding not be addressed promptly. This includes matters that involve significant non-compliance with legislation and/or policy.
	**Moderate** finding include those matters which, while not necessarily individually significant, are of sufficient concern to warrant action being taken by the agency as soon as practicable.
	Minor finding include those where the finding is not of primary concern but, in the interests of the entity, still warrant action being taken to remedy the matter.
	No findings reported.

The detailed results of our audit are summarised below on an agency by agency basis.

Department of Fisheries

The Department of Fisheries (Fisheries) have adopted the software as a service (SaaS) model for the cloud based service that supports their Commercial Vessel Monitoring System (VMS). The system is used for the real-time monitoring of approximately 260 boats across 22 commercial fisheries off the Western Australian coast. Commercial fishing is a significant operation that contributes in excess of $300 million per year to the WA economy. In this arrangement the main vessel monitoring application is provided by one service provider. The servers hosting the system and supporting infrastructure are housed in another service provider's data centre. This data centre and the servers are located in Sydney. Figure 2 provides a basic overview of this service.

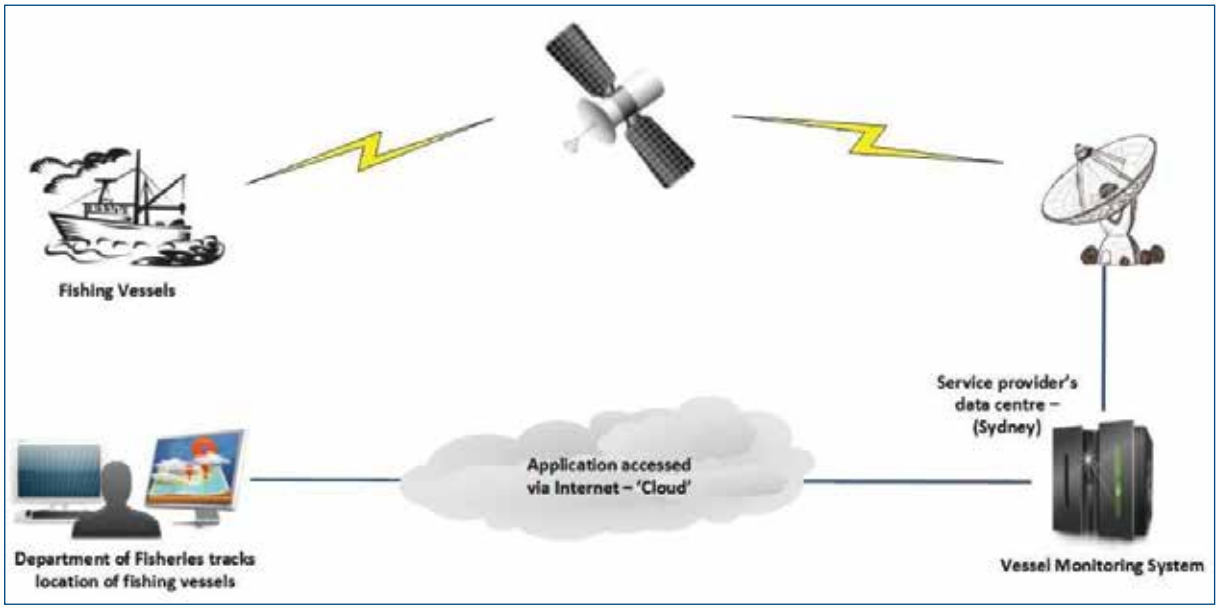

Figure 2: The Department of Fisheries uses the cloud to support its monitoring of commercial vessels

This complex system provides a critical function, however Fisheries had not identified the risks related to their decision to implement this arrangement or thereafter assessed and treated these risks. The risks include unauthorised access to commercially sensitive fishing information, system disruptions or the complete loss of service. Should these risks occur they could have a serious impact on the State's commercial fishing operations and Fisheries' ability to monitor fishing vessels for compliance with area restrictions.

Fisheries proceeded with the cloud solution without completing an adequate business case that included consideration of the above risks. Without a sound business case, Fisheries was unable to show that they fully considered all potential options to arrive at the most effective solution. It is also unlikely that they had a clear understanding of the service benefits and how these were going to be achieved.

Although the VMS provides a key service, the contract with the system provider is missing some important terms and conditions to protect Fisheries' interests. For example:

- Fisheries had not adequately defined its security requirements and included these in the contract

- the service provider was not required to regularly report to Fisheries on the system security controls that are in place and of auditing that will be done of the effectiveness of the systems security controls
- the responsibilities and actions of both parties in the event of the service terminating is not detailed.

We also found that Fisheries was not receiving regular service or security reports from the service provider, which is a requirement of the contract service level agreement. The information in these reports is essential to alerting Fisheries as to whether it is exposed to a poorly performing and insecure service.

Fisheries did not have an information security policy of their own to assist them to define the security requirements they required in the contract with their provider. This contributed to a number of weaknesses in the system and service provider operations, such as:

- information was not securely deleted from hard drives before they were disposed of or re-used. This increases the risk that the information on these disks can be recovered resulting in unauthorised access or disclosure
- the data on the backup tapes was not encrypted. The lack of encryption makes it easier for anyone with access to the tapes to read the information
- auditing of login failures on the system had been turned off. As a result, it is less likely that attempts to gain unauthorised access to the system would be quickly detected.

The VMS provides a key service to Fisheries. However, it does not have a business continuity plan (BCP) to enable continued vessel monitoring in the event of an incident affecting the cloud service or if the provider ceased operations. A BCP would reduce the impact that an incident or cessation of the providers operations would have on Fisheries operations.

Public Transport Authority

The Public Transport Authority (PTA) has acquired a software service to process Transwa regional coach and rail bookings. Customers can make their travel bookings directly online (https://www.transwa.wa.gov.au) or via the authority call centre or through a regional agent.

The main application that processes bookings is provided by one service provider. The servers that run this application and store the PTA and customer information are owned and managed by a second service provider. The servers are housed in two data centres both located in Sydney which are owned and managed by a third service provider. The payment of bookings involves an interface with a card payment gateway. The payment gateway is provided by a fourth service provider and runs on servers in a different data centre. Figure 3 gives a basic overview of this arrangement.

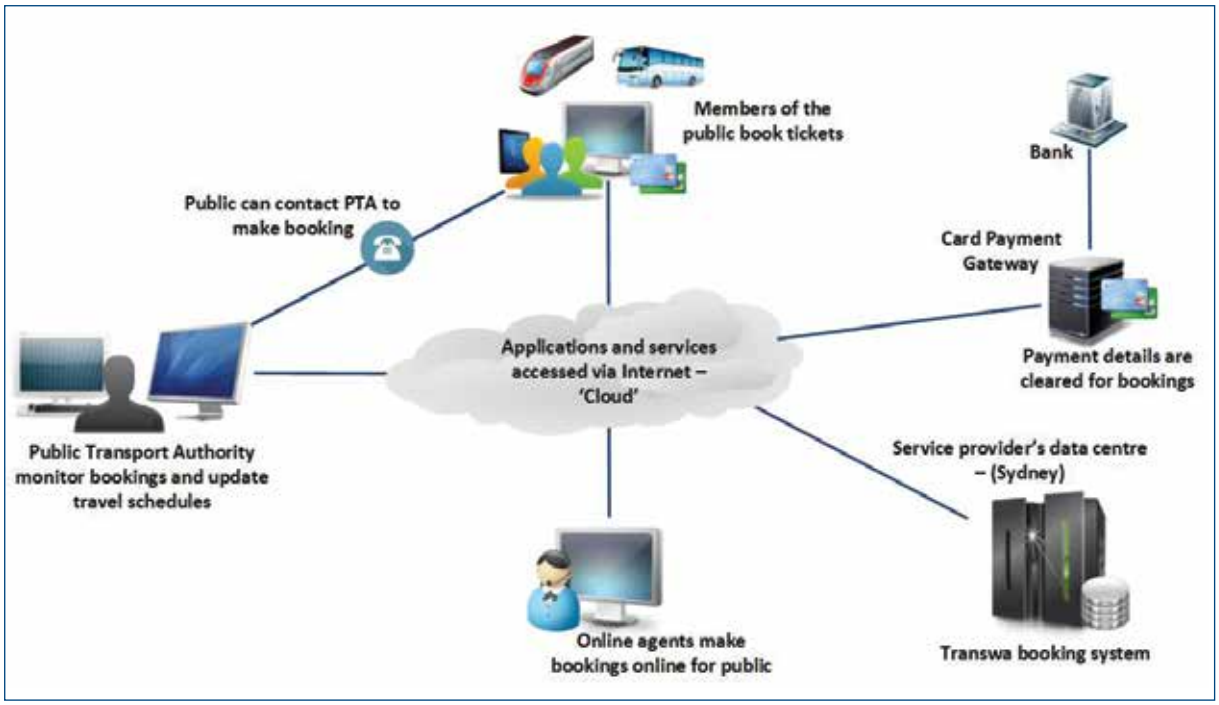

Figure 3: The Public Transport Authority uses the cloud to support its regional coach and rail travel bookings

Despite the complexity of the service and the sensitivity of the customer information being processed, the PTA had not identified or managed the risks related to these arrangements. The risks include; unauthorised access to customer information, system interruptions, complete loss of service and data being offshored. Emergence of these risks could impact on customer's personal information and travel arrangements.

We noted that the PTA had not adequately defined and communicated their information security requirements to the service providers through the contracts.

These security requirements instruct the service provider and any sub-contractors on the security controls that should be in place to protect PTA and customer information. The absence of these requirements means that there is no contractual constraint to prevent customer information being stored on computer systems located overseas. The PTA had also not stipulated how long they required the customer and booking information to be stored and retained on the service providers' IT systems. By not defining and communicating their data security requirements to the service provider, there is an increased risk to the confidentiality, integrity and availability of the PTA's information.

The PTA and their main service provider did not have any business continuity or disaster recovery plans (DRP) to cover the continued operation of the system which is critical for booking and managing regional travel. A BCP and DRP would reduce the impact that an incident or cessation of the providers operations would have on the PTA and on those members of the public wishing to travel.

Public Sector Commission

The Public Sector Commission (Commission) has acquired a recruitment portal software service. This portal provides a centralised website (www.jobs.wa.gov.au) for positions in the WA public sector. Agencies use the service to advertise their vacancies and manage applications for those roles. It also provides the public with a central view of all vacancies and enables them to submit their job applications online. The recruitment portal application is provided by one

service provider. The application is located on servers in a Sydney data centre which is owned and managed by another service provider. Figure 4 provides a basic overview of this service.

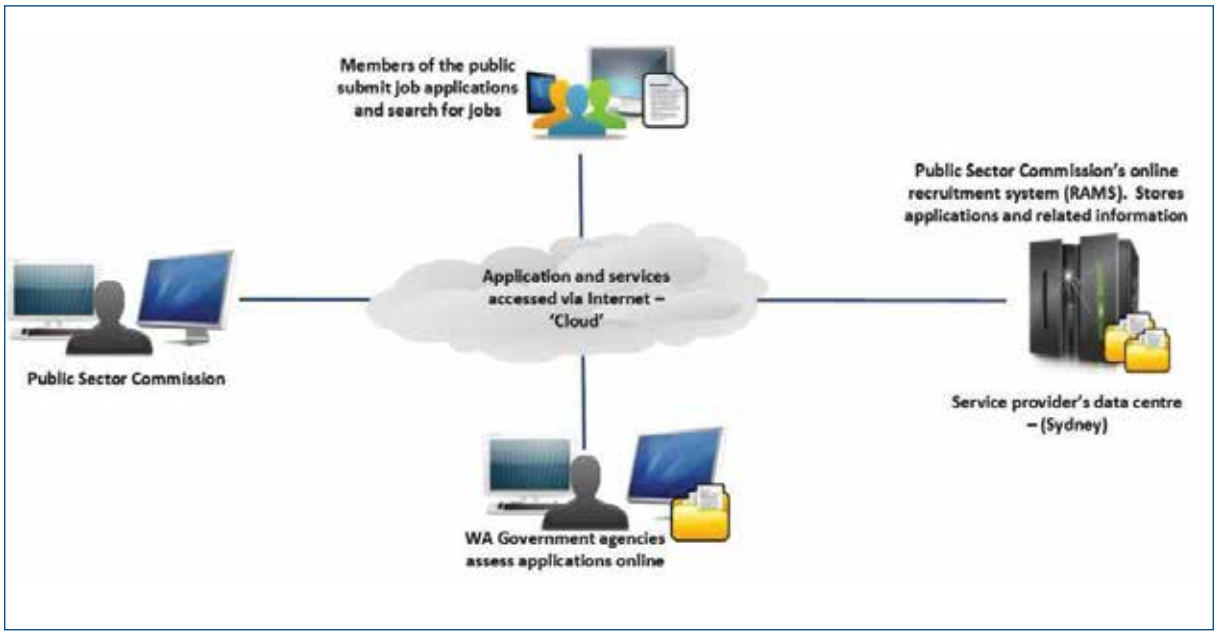

Figure 4: The Public Sector Commission uses the cloud to support recruitment across the WA public sector

The contractual arrangement between the Commission and the service provider is missing key security terms and conditions to ensure the confidentiality of sensitive and personal information the system stores and processes. These include:

- no defined requirement for data encryption to protect personal information
- no requirement to ensure data is securely deleted from surplus media (e.g. tape, hard disk or CD-Rom)
- inadequate reporting requirements defined for the Commission to gain assurance on system security
- inadequate provision for auditing the design and effectiveness of security controls.

We also noted that the service provider had not implemented an appropriate intrusion detection system (IDS). An IDS would help detect any cyber attacks aimed at taking the system offline or gain unauthorised access. In addition, the service provider was not completing any vulnerability assessments on the system and network. Regular assessments allow system or software weaknesses and vulnerabilities to be identified and addressed to prevent exploitation by hackers or cyber criminals.

The Commission did not have a business continuity plan to cover the continued operation of the service. This increases the risk that the recruitment system will not be available for an extended period of time if there is an unplanned incident or the service provider ceases operation. The Commission had also failed to gain assurance from their service provider that they had adequate disaster recovery plans in place. Without effective and tested continuity and recovery plans there is an increased risk to the overall availability of the service. This could impact the state government's ability to manage staff recruitment.

Department of Sport and Recreation and Metropolitan Redevelopment Authority – Talent2

Both the Department of Sport and Recreation (DSR) and the Metropolitan Redevelopment Authority (MRA) were using 'software as a service' (Talent2) to manage and process their staff pay and other benefits.

Talent2 is a cloud based HR system in common use amongst WA government agencies. The Department of Finance entered into a common use arrangement to deliver Talent2, for agencies in 2002. When the contract recently expired, individual agencies were required to negotiate their own arrangements.

Both DSR and MRA took a decision in 2013 to extend their contract with the service provider without fully considering alternate options or whether the terms of the agreement were still relevant. We acknowledge that the time frame to do this was very limited due to the government's decision not to proceed with the Shared Service arrangements across the sector. Due to the short time frame agencies had limited capacity to determine whether the cloud based arrangement best suited their needs. However given the sensitivity of the personal information being stored on Talent2, all agencies should ensure they have a full understanding of the contract and service levels (security, quality and availability) they are accepting.

We noted a number of issues in relation to the Talent2 arrangements that had potential to result in unauthorised access to personal information or in staff not being paid:

- the service provider stores back-up copies of information in Melbourne whilst the contractual arrangements stipulate that data should only be held in Western Australia
- neither agency was monitoring key performance criteria set out in the contract. This included security, quality and availability of the service
- the Department of Sport and Recreation had not developed a business continuity plan to ensure the ongoing operation of the service following an unplanned event.

Metropolitan Redevelopment Authority – Infrastructure as a Service

In addition to Talent2, the MRA has also implemented an 'infrastructure as a service' (IAAS) model. Under this arrangement, all of the MRA's computing resources and supporting ICT infrastructure is hosted from a service provider's Perth based data centre.

Our audit of these arrangements identified weaknesses in the MRA's process for managing its cloud based risks. These weaknesses could result in commercially sensitive information being exposed to unauthorised access or disclosure or could affect the availability of key information on metropolitan redevelopment projects. The weaknesses included:

- the MRA adopted a cloud solution for their ICT infrastructure without completing an adequate business case and without a documented analysis of its risks
- a range of key terms and conditions covering areas such as security, performance and auditing were missing from the contract
- gaps in key security controls. These related to fixing known security vulnerabilities and securely deleting information from hard drives before disposal or re-use
- the MRA did not have an adequate business continuity plan. Details of what actions they planned to take to continue their IT operations should the service provider suffer a significant outage or cease operating were unclear. In addition, they had not defined or agreed any disaster recovery arrangements with their service provider.

Appendix 1 – Central agency views about the use of the cloud

We sought advice from the State Records Office and the Information Commissioner about their views on the use of cloud computing within government agencies.

The following is a summary of their advice.

State Records Office

The State Records Office (SRO) of Western Australia is the Western Australian public records authority with responsibility for managing, preserving and providing access to the State's records.

The SRO is of the view that although there are potential benefits for government agencies utilising cloud computing there are a number of risks that should first be properly assessed.

The major issues in relation to records and information management which agencies need to consider and mitigate when considering cloud computing include, but are not limited to:

- risk of loss of access to their information
- risk of unauthorised access to their information
- unauthorised destruction of their information
- security and protection of their information
- custody and ownership of their data and information.

To assist agencies in assessing whether a cloud computing arrangement is appropriate to its business operations, the Australasian Digital Record Keeping Initiative (ADRI) guideline *Advice on managing the recordkeeping risks associated with cloud computing* is available from the SRO website. ADRI is a working group of the Council of Australasian Archives and Records Authorities and, as a member organisation, the SRO endorses the risk assessment approach in the guideline.

The SRO is also developing a new guideline to provide information management advice on cloud computing specific to WA government agencies and to complement the Cloud Computing suite of tools currently being developed by the Department of Finance.

Information Commissioner

Agencies considering or using cloud based services need to factor the requirements of all applicable legislation, including the *Freedom of Information Act 1992* (FOI Act), into the early stages of any planning or procurement process.

The use of cloud based services is not inherently incompatible with the FOI Act, as the Act gives the public a right to access all documents (including electronic documents in any form) which are in the possession or under the control of an agency. This includes documents which an agency is entitled to access, even though they may not be in the agency's physical possession.

However, failing to take the requirements of the Act into account at the planning stage can lead to a situation where the objects of the FOI Act are frustrated in practice. For example, it may be more difficult or costly to undertake reliable and comprehensive searches for all documents which may be within scope of a particular FOI application. Depending on a service provider's data and cost structure, retrieval of documents may also be delayed or rendered

more costly due to complex extraction procedures. Conversely, the well-planned and executed use of cloud services may enhance the ability of an agency to achieve the objects of the FOI Act, by allowing for efficient and effective searches across all relevant data holdings and speedy retrieval, especially where this replaces or interconnects previously incompatible and distributed systems.

Agencies also need to ensure that cloud based services provide acceptable levels of data security and integrity to allow the agency to comply with all of its oversight and accountability obligations, including those under the FOI Act.

The most important point is to consider and address these issues at the early stages of planning and to be aware of the practical impact which system design can have on an agency's ability to achieve the FOI Act's legislative objects of greater public participation in government and improved government accountability.

Application Controls Audits

- Management of Water Pipes Applications – Water Corporation
- Management of Wood Pole assets Applications – Western Power
- Local Area Data Set and Provider Administration and Information Data Applications – Disability Services Commission

Management of Water Pipes Applications – Water Corporation

In February this year we reported on the Water Corporation's Management of Water Pipes[2]. In that report we identified gaps in the Water Corporation's information that needed to be addressed to ensure pipe replacement decisions are fully informed. This report provides more specific information about some of the IT applications that support the Water Corporation's management of water pipes.

Conclusion

In general, the five water supply pipe applications we assessed enabled the Water Corporation to adequately manage aspects of the water supply network.

However, we identified control weaknesses relating to the completeness and accuracy of information on the condition of water pipes that is entered through the MDS system and which ultimately affects the reliability of the information held in the SAP system. In the absence of accurate and reliable information, the Water Corporation's ability to effectively manage water pipes is reduced.

In addition, we found staff had different views about how the various applications link and share information. One cause of this is that the Water Corporation did not have an appropriate Enterprise Architecture diagram for the applications and systems that support the management of their water pipe systems. This diagram would provide an overview of their systems and how they interoperate. It also shows workflow and data entry points which will assist with risk identification and improvement opportunities.

Background

In 2012-13 the Water Corporation supplied over 357 billion litres of drinking water across Western Australia. To deliver this water the Water Corporation manages over 34 000 kilometres of water supply pipes across the state.

Approximately 20 applications and processes are used for the management of water supply pipes. This audit assessed the five main applications:

Systems, Applications and Products (SAP)

This system is used to manage a wide variety of water supply pipe information. This includes pipe installation, refurbishment, replacement dates and a schedule of water pipe maintenance work.

Supervisory Control and Data Acquisition (SCADA)

This is a variety of computer systems and devices used to monitor water quality including management of pumps and valves for the supply of water throughout the state.

Facilities Mapping System (FMS)

This is a Geographical Information System (GIS) used to specifically locate water pipe infrastructure on a map with relevant detail.

2 Water Corporation: Management of Water Pipes. Report 1, February 2014.

GRANGE (Customer Management System)

This application is the initial entry point for recording faults and incidents. The system also records details of the person reporting the fault or incident and related details.

Mobile Device System (MDS)

Field staff working on location use this system which sends and receives data about the condition of water pipes and work orders. Field staff respond to issued work orders and enter information through mobile handheld devices.

Key Findings

High level view of water supply pipe applications

The Water Corporation advises that it has a clear picture of its enterprise architecture although this would not usually be broken down and focused on an asset class (e.g. water pipes). It thus did not have a sufficiently detailed high level picture of its critical applications, system interfaces and information flows related to the management of water supply pipes. The systems used to manage the water supply pipes have evolved over time with the addition of new applications and modules to help improve the management process. The environment is now very complex and there is uncertainty amongst key staff about how the various systems interrelate. Without a good understanding of how the different applications interrelate, it is difficult for management to identify where potential risks exist or areas for improvements can be made.

Integrity and accuracy of water pipe information needed improvement

The Water Corporation has a variety of issues that affect the integrity and accuracy of the water supply pipe information.

Operational staff reported that work order information entered into the MDS by field staff routinely contained errors or is not entered. Data we analysed confirmed the occurrence of errors and incomplete information. The problem for the Water Corporation emerges when the error feeds into the SAP system, which harms its understanding of the condition of its water supply pipes.

FMS is the Water Corporation's primary source of information about the age of pipes. We reported earlier this year[3] of errors found in the recorded installation dates of old pipes in the Perth CBD. The errors came to light after an incident in Wellington Street in April 2013 when a cast iron pipe burst three times in one week. A data quality review found these pipes were in excess of 100 years old rather than the 60 to 70 year range recorded in the FMS. The Water Corporation subsequently verified the age information for all cast iron pipes in the Perth CBD and now plans to undertake data quality reviews for similar aged pipes in Fremantle, Guildford, Northbridge and Victoria Park.

Data integrity and accuracy issues have a negative impact on the efficiency of staff and business operations. These issues also increase the risk that mistakes and incorrect decisions will be made. Despite knowing about these problems the Water Corporation has very limited processes to review and validate the accuracy of water supply pipe information entered into the systems.

3 Water Corporation – Management of Water Pipes – February 2014.

We noted that the Water Corporation has identified data integrity as a high risk item in their risk register and a project is underway to improve data integrity throughout their systems.

System inefficiencies result in time consuming manual processing

We observed that the Water Corporation relies on manual processes to manage the water supply pipe information. Rather than data being maintained in a centralised system or information being automatically linked across systems, staff have to manually track and update the information.

In one instance we noted staff having to copy and paste control system alarm responses from SCADA into SAP to generate maintenance work orders. In another example we noted the GRANGE system does not prevent duplicate work orders from being entered for the same fault. As a result, staff have to manually check a shared Microsoft Outlook Calendar to see if a work order for the fault had already been created.

Manual processing is inefficient and time consuming. It also increases the risk of data being entered incorrectly which in turn could lead to incorrect business decisions affecting system reliability and costs.

System reliability and availability impacts business operations

There were a range of issues affecting the overall reliability and availability of the Water Corporation's water supply pipe systems. For instance:

- the interface between GRANGE and SAP was poorly configured and susceptible to information transfer failures. Management advised that failures occur regularly causing delays in issuing work orders for water infrastructure maintenance and correction of faults
- the Water Corporation's IT group carries out system maintenance during busy periods resulting in the SAP system being unavailable to log fault calls. During system maintenance periods staff have to record work orders manually on paper which results in a large backlog in the processing of work orders. When the systems become available, up to three additional staff are required to process the backlog.

Reliability and availability issues increase the risk that key business operations or activities will be impacted, which can affect staff efficiency, increase costs and cause errors in data input.

Security over sensitive information

We established that by default all Water Corporation staff have been given read access to large amounts of sensitive information stored on one of their systems. This includes census data, customer account information and other government agency information. Granting this broad level of access to information increases the risk of unauthorised disclosure or misuse.

Recommendations

The Water Corporation should by the end of 2014 commence action to address the following recommendations:

- Develop an enterprise architecture diagram to provide visibility of applications, interfaces and processes that support the management of water supply pipes. The diagram then needs to be regularly maintained and updated.
- Based on a full understanding of the architecture, address the following areas in a systematic way to maximise benefits and minimise risks:
  - Identify and address key areas to improve the integrity and accuracy of data held on their systems. This work should be sufficiently resourced to ensure areas for improvement are addressed within a timely manner.
  - Implement automated processes and interfaces where applicable, to help ensure the timely transfer of accurate information between systems.
  - Complete a review of each business area's application availability and reliability requirements. Where appropriate, applications should be configured and/or fixed to ensure they meet business requirements. Consideration should also be given to scheduling maintenance windows of a shorter duration or at less busy periods when work order volumes are lower.
  - Undertake a review of user access privileges to the system which we identified as allowing broad access to the sensitive information the system contains. As part of this review, relevant controls should be implemented to prevent or detect unauthorised information access or disclosure.

Agency Response

The *Water Corporations Act 1995* requires the Corporation to act in a commercial manner and must take this into account when spending on systems and integration between systems. This being said, the Corporation will act on the findings as outlined in our response to the management letter.

Management of Wood Pole assets Applications – Western Power

In November 2013 we reported on Western Power's Management of Wood Pole Assets[4]. In that report we identified that Western Power still needed to make progress to ensure its data collection is complete and accurate. This report provides more specific information about some of the IT applications that support Western Power's management of it wood pole assets.

Conclusion

The applications we assessed generally enabled Western Power to adequately manage its wood pole assets.

However, we identified control weaknesses that impact on the accuracy and integrity of asset maintenance information entered through the DMS system. These weaknesses affect the reliability of the information held in the Ellipse system. In the absence of accurate and reliable information, Western Power's ability to effectively manage its wood pole assets is reduced.

We also found that further work was required to ensure Western Power had clear end to end visibility over the applications that make up the wood poles management system.

Since this audit was completed late last year, Western Power has advised that they have undertaken a detailed review of their end-to-end organisation, processes, systems and work practices. This review has led to a number of actions designed to drive improved operational performance and are being completed within the context of a broader business program.

Background

Western Power transports and delivers electricity to the south west corridor of Western Australia. Its network is made up of 42 000 transmission towers and poles that transport electricity from generators to substations, and 758 000 distribution poles delivering electricity from substations to consumers. There are approximately 629 000 wood poles in the network.

The information technology system to manage the wood poles infrastructure has expanded and developed over time and currently comprises around 15 applications. This audit assessed the five main applications:

Ellipse

This system manages all the work orders and the equipment register (asset management) and is the core financial system.

ADAPT

This system is used to verify the equipment defects and generates work order requirements prior to loading into Ellipse which subsequently creates the work order.

Document Management System

This is a document management system used between Western Power and contractors undertaking work on their behalf. It is used to transfer the invoices between third party contractors and Western Power as well as communication of work orders.

4 Western Power's Management of its Wood Pole Assets. Report 17, November 2013.

COGNOS

COGNOS is the reporting layer used to consolidate information and generate reports such as KPI's and monthly performance management reports.

Handheld Device System

Field staff working on location use this system to send and receive data about the condition of wood poles and work orders. Field staff respond to issued work orders and enter information through mobile handheld devices.

Key Findings

High level view of wood pole management applications

Western Power advised it has a clear picture of its enterprise architecture and IT application landscape, allowing the effective management and governance of end-to-end IT solutions. Whilst this enterprise architecture would not usually be broken down and focused on asset class (e.g. Wood Poles), there is value in further work to ensure specific end-to-end visibility over the IT applications focused on Wood Pole Management. This will mitigate the risk of inefficiency in their use and support of Wood Pole Management and the risk that changes in one process / application has a detrimental impact on other processes or components within the system.

The system used to manage the Wood Poles infrastructure has evolved over time with the addition of new applications and modules to help improve the management process. We observed that the environment is now very complex with no overall (end to end) visibility over data input sources and transfers of information between the applications which make up the Wood Poles management system. Failure to maintain visibility over the makeup of the Wood Poles management system and full data flow increases the risk that there is inefficiency in its use and support. There is also a risk that changes against one process / application has a detrimental impact on other processes or components within the system.

Augmenting the enterprise architecture approach already in place to provide end to end visibility over the applications making up the Wood Poles management system, along with the flow of data and key control points, would help management simplify and manage the confidentiality, integrity and availability of data within, and flowing through the system.

Integrity and accuracy of wood pole asset information

Western Power need to address a number of issues that could potentially affect accuracy and integrity of data within the system used to manage Wood Poles.

We found that asset maintenance work, including replacement and maintenance work on Wood Poles and its components, is allocated using an insecure file in the Document Management System (DMS). The data is then sent to and can be edited by multiple third parties who perform the allocated maintenance work. On completion of the maintenance work, the job information is uploaded into Ellipse to close the work orders. This information is at risk of being fraudulently or accidently amended under the current process. A more secure method of sharing information with third party service providers will help maintain the confidentiality, integrity and availability of the data for incorporation back into the Ellipse system.

Each Wood Pole asset is made up of a number of components including the pole itself, the cross arm and transformer. When the pole is replaced these are also replaced. We noted that the ADAPT application, used as part of the work scheduling process, does not link some

of the larger component items to the pole when it is selected for work. As a result, when the pole is replaced these component items are not updated through the standard process. A manual work around was required to capture and amend the linked items. Ensuring that the components are effectively linked to the poles will help Western Power maintain a more accurate record of assets and works required and eliminate the need to manually track and record the replacement of component parts.

Unnecessary work orders are created

The collection of data pertaining to Wood Pole inspections is captured on hand held devices by the inspector at the time of inspection. If a pole is inspected whilst a work order remains outstanding, the pole identification number will be available in the hand held device. If the inspector attempts to raise a secondary defect, the system will alert them that there is still a defect outstanding. If however the inspector considers the pole unserviceable and raises a replacement request, there is no such alert. This replacement request and the original work order are both reflected in Workplanner. Failure to implement controls to reduce multiple defect or replace entries against the same asset increases the risk that multiple work orders are generated and multiple visits made where no action is required.

Manual reporting processes increase the risk of errors in reporting

The wood pole management reporting model gathers performance data from multiple systems. This data is consolidated into a master spreadsheet which is used to derive monthly management reports which includes the current status of the wood pole replacement program. We noted that there is a significant amount of manual intervention and data entry required once data leaves the systems, and extensive use of spreadsheets to generate the monthly management reports. These manual processes increase the risk of errors or unauthorised changes. Minimising the amount of manual intervention required to generate reports will help streamline the reporting process and enhance the integrity of the reports.

Recommendations

Western Power should by the end of 2014 commence action to address the following recommendations:

- Augment its existing approach to enterprise architecture management to develop a diagram that provides specific visibility of applications, interfaces and processes that support the management of wood power poles. The diagram then needs to be regularly maintained and updated.
- Based on a full understanding of the architecture, address the following areas in a systematic way to maximise benefits and minimise risks:
  - Identify and address key areas to improve the integrity and accuracy of data held on their systems. This work should be sufficiently resourced to ensure areas for improvement are addressed within a timely manner.
  - Implement automated processes and interfaces where applicable, to help ensure the timely transfer of accurate information between systems and streamline the monthly management reporting process.

Agency Response

Western Power accepts the findings of the audit and would like to express its thanks to the Office of the Auditor General (OAG) for its efforts and advice.

Overall the OAG concluded that Western Power's applications generally enabled it to adequately manage its wood pole assets.

In response to the two recommendations highlighted;

1. A diagram focused specifically on the applications supporting the management of Wood Power Poles has been created and is being maintained accordingly. This is being done within the context of Western Power's broader approach to managing its enterprise architecture and IT applications.

2. A detailed assessment of Western Power's end-to-end processes, systems and work practices has been completed. This review has identified a range of improvement areas in regard to the integrity and accuracy of data, and the automation of processes and interfaces.

Western Power has commenced work to implement and sustain these improvement areas as part of a broader business program to improve the performance of key end-to-end processes, systems and work practices.

Local Area Data Set and Provider Administration and Information Data Applications – Disability Services Commission

Conclusion

Both the Local Area Data Set (LADS) application and the Provider Administration and Information Data (PAID) application were operating as designed.

However, the LADS application was affected by a small number of control weaknesses mainly relating to the integrity of client data while PAID is an ageing application which doesn't support all of the Disability Services Commission's (Commission) current processes. We do not regard these issues as critical but they do somewhat reduce the efficiency of staff and the Commission's business operations and moderately increase the risk of fraudulent activity or payment errors.

Background

The Commission helps people with disabilities to live in the community. They also provide help and support to the families and carers of people with disabilities. The Commission achieves this by providing services through specific funding to an individual or disability support organisations.

This audit assessed two applications that facilitate the payment of funding assistance to individuals and support organisations:

- The LADS application is used to manage direct payments to people with disabilities, members of their family or a carer. In 2012-13, LADS managed support payments of approximately $28 million to nearly 10 000 individuals.
- PAID is used to manage payments to about 120 disability support organisations. In 2012-2013, PAID processed payments of around $497 million to these organisations.

The LADS and PAID applications provide payments for the following types of support services:

- accommodation for people with challenging behaviour
- care advice and respite for families and carers
- financial advice, including government payments and benefits
- health and well-being advice on key services
- planning for individuals to achieve goals at various stages in life
- housing, working and training, transport, recreation and leisure advocacy information and planning support.

Key Findings

LADS

Although we found that LADS is working properly, there are two issues that should be addressed.

Existing payment recipients did not always appear on the payment screen of the LADS application and could therefore not be selected for a fresh payment. To address this fault the Local Area Coordinator has to manually re-enter the recipient details as a new record. This results in an unmatched payment request in the financial system. Since 1 July 2009 there have been 4 325 unmatched payment requests, which have to be manually processed. This problem creates an additional overhead cost and increases the risk of fraud and errors.

A flaw in the system inappropriately provided access to some system users to change sensitive client information such as legal name and date of birth. This increases the risk of fraudulent changes and may impact the overall integrity and accuracy of the Commission's client information.

PAID

The PAID application is working adequately, but it is an ageing system that does not fully support all the business processes associated with paying the disability support organisations.

The Commission has implemented several manual processes to assist in managing their payments to disability support organisations, but these can be inefficient and are a cause of delays to the processing of payments. The lack of full automation also increases the risk of unauthorised changes, errors or fraudulent activity.

Some examples are:

- The system does not record payment approvals in accordance with manual approval delegations. This is due to the systems limitation of only being able to record the first level of approval
- A log is not kept of information changes made in the system about a disability support organisation. Such changes could, for instance, include postal address and bank account details. A log provides a record of who made the changes and when.
- Some Commission staff have been given Administrator level access to the system to enable them to extract information to prepare management reports. Administrator level access is a high level of privilege that is normally restricted to a minimum number of staff because it generally allows users to make significant changes to data and to how the application functions.

Recommendations

The Disability Services Commission should within three months take action to address the following recommendations.

- For the LADS application:
  - determine why certain payment recipients are not available for selection and then apply a suitable application fix or update
  - ascertain how some system users can change sensitive client information and then apply a suitable application fix. Until the issue is resolved, the Commission should implement stringent controls to prevent or detect any unauthorised changes to information.
- For the PAID application:
  - undertake a review of the system capabilities against the supporting business processes. This review should determine whether current application functionality meets their business requirements. Based on the outcome of this review the Commission may consider making relevant application modifications or changes to their processes. The Commission may want to evaluate updating or replacing the PAID application.

Agency Response

The Commission has welcomed and accepts all these findings.

The Local Area Data Set (LADS) system software error has been corrected and the Manual Payment Input issue is currently being addressed. The Provider Administration and Information Database (PAID) system is recognized as having inadequacies and using old technology.

Having said this, the Commission is developing and implementing a new system to support the introduction of the State's National Disability Insurance Agency (NDIA) trials in Western Australia. The trials were committed by the Prime Minister and the Western Australian Premier through a bilateral agreement signed on 31 March 2014. The trials are scheduled to begin on 1 July 2014 for a two year period. A comparative and independent valuation of the trial outcomes will be conducted.

The Commission is fully committed to providing an operational environment that will support the future directions of disability services. The new NDIA-My Way system will overcome some PAID deficiencies but until there is certainty around the NDIS, the Commission will continue to utilise manual processes to remediate the remainder rather than invest in the PAID system development.

Therefore, the Commission cannot action the requested recommendations from the Auditor General at this time, due to practicality and unknown business requirements which will be dependent upon a national reform process underway.

General Computer Controls and Capability Assessments

Conclusion

We reported 455 general computer controls issues to the 54 agencies audited in 2013.

From the 42 agencies that had capability assessments conducted only eight were meeting our expectations for managing their environments effectively. More than half of the agencies were not meeting our benchmark expectations in three or more categories. Nevertheless, the overall result was a slight improvement on the prior year.

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

Background

The objective of our general computer controls (GCC) audits is to determine whether the computer controls effectively support the confidentiality, integrity, and availability of information systems. General computer controls include controls over the information technology (IT) environment, computer operations, access to programs and data, program development and program changes. In 2013 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 54 agencies and completed capability assessments at 42 of them. This is the sixth 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[5] 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)

The graphs and tables that follow show in green the percentage of agencies that attained at least a level three in the rating criteria. Red indicates that they were below level three.

What did we find?

Our capability maturity model assessments show that agencies need to establish better controls to manage their IT operations, IT risks, Information security and Business continuity. Figure 2 overleaf summarises the results of the capability assessments across all categories for the 42 agencies we audited. We expect agencies should be at least within the level three band across all the categories.

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

Figure 1: Capability Maturity Model Assessment Results

The model shows that the categories with the most weakness were management of IT risks, information security and business continuity.

The percentage of agencies reaching level three or above for individual categories was as follows:

	2013	2012
IT operations	64 per cent	58 per cent
Management of IT risks	50 per cent	44 per cent
Information security	40 per cent	44 per cent
Business continuity	36 per cent	25 per cent
Change control	69 per cent	69 per cent
Physical security	86 per cent	75 per cent

Table 2: Percentage of agencies attaining at least level three

There was an improvement in four areas from the previous year. Information security declined by four per cent and Change control remained the same.

Eight of the 42 agencies were assessed as level three or above across all categories which is an improvement from only three agencies achieving this from the previous year. More than half of the agencies did not achieve level three rating for three or more categories.

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

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

IT Operations

This is the third year we have assessed IT Operations for agencies. There was a six per cent improvement by IT branches in IT practices and the service level performance provided to meet their agency's business requirements (Figure 2).

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.

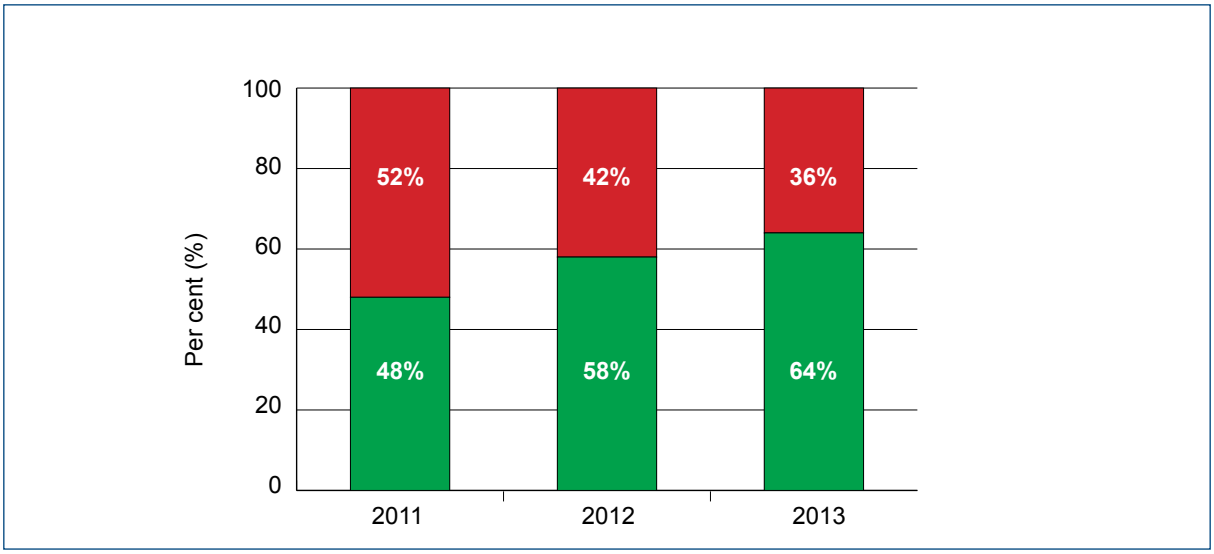

Figure 2: IT Operations

Examples of findings:

- Several agencies that require staff to sign a confidentiality declaration or non-disclosure agreement had failed to collect or retain these documents.
- A number of agencies do not have adequate processes in place to review security logs generated by core systems and infrastructure. Examples include:
  - logs for remote access systems
  - modifications made to databases containing confidential information
  - alerts from automated security systems
- A number of agencies have either no, incomplete or out-dated Information Security Policies
- One agency had inconsistent and incorrect incurring limits within their expense management system.

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

Management of IT risks

Fifty per cent of agencies met our expectations for managing IT risks, a six per cent improvement on the previous year.

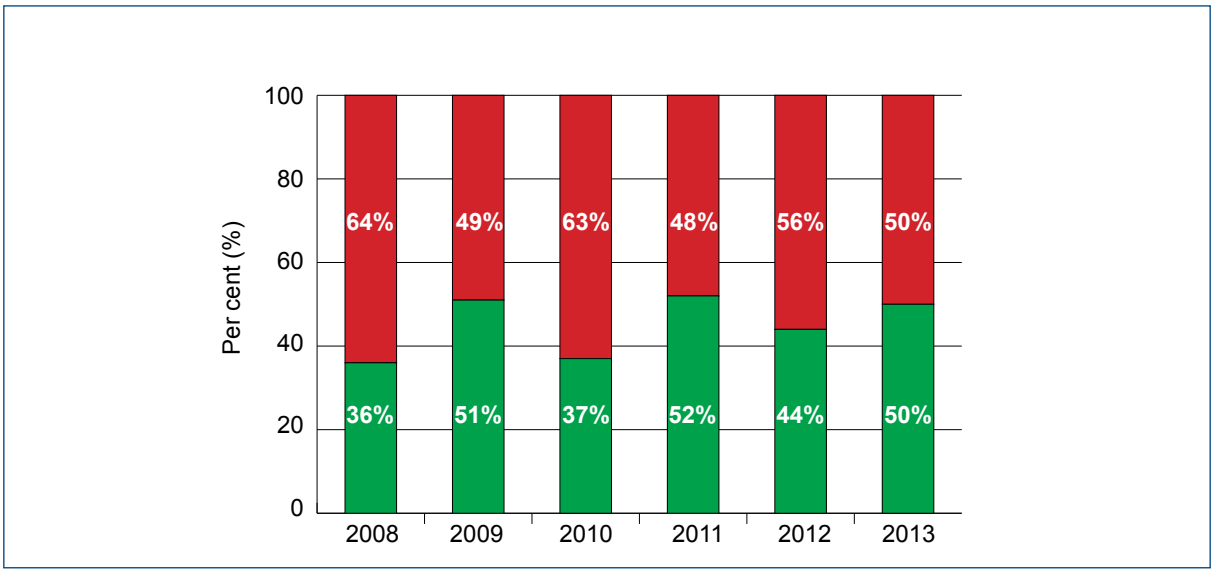

Figure 3: Management of IT Risks

Examples of findings:

- a number of agencies did not have a risk management process for identifying, assessing and treating IT and related risks. Also many agencies still do not have a risk register for ongoing monitoring and mitigation of identified risks
    - one agency has insufficiently or inaccurately recorded IT risks in the risk register. Key details such as the level of risk and compensating controls were misrepresented
- one agency's IT risks identified within their risk register have not been reviewed since 2009 to ensure the relevance of the risks and associated plans.

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

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

Information security

Only 40 per cent of agencies met our benchmark for effectively managing information security, down four per cent from the previous year. 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.

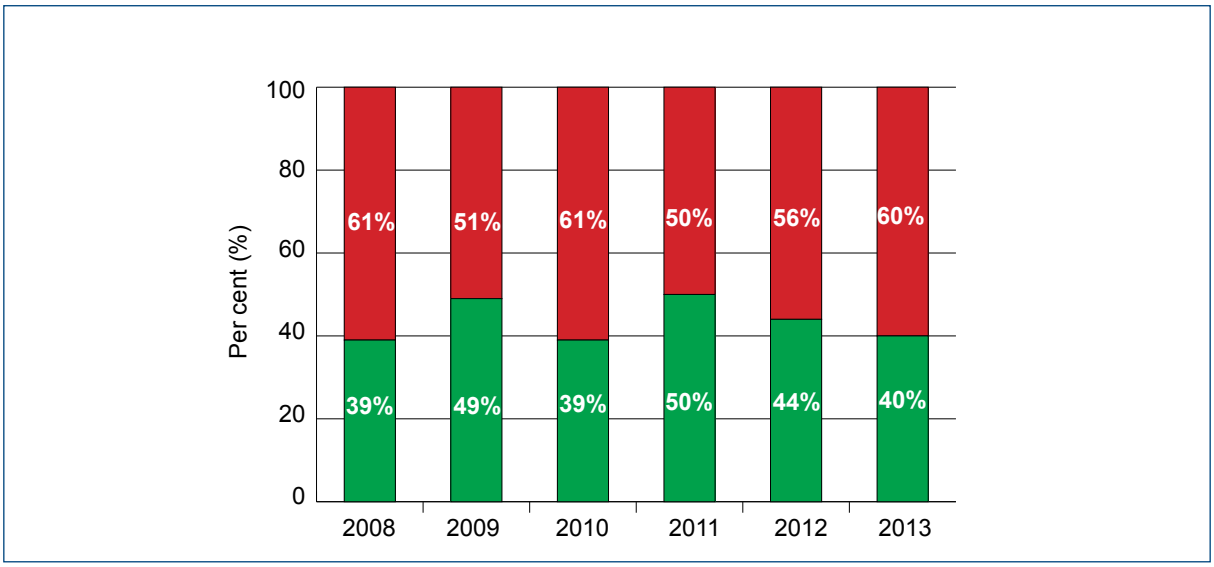

Figure 4: Information Security

Examples of findings:

- we found weak password settings with one agency allowing network user accounts with passwords such as 'aaaaaa'
- agencies did not have effective process in place to identify potential security vulnerabilities across their IT infrastructure in a timely manner. We ran our own vulnerability scans and found examples in multiple agencies where critical and moderate security issues were identified
- a number of agencies did not have good processes in place to review application and network accounts. We found one example of an agency with over 2000 generic user accounts.

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 a 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 an 11 per cent improvement from last year but 64 per cent of the agencies still did not have adequate business continuity arrangements.

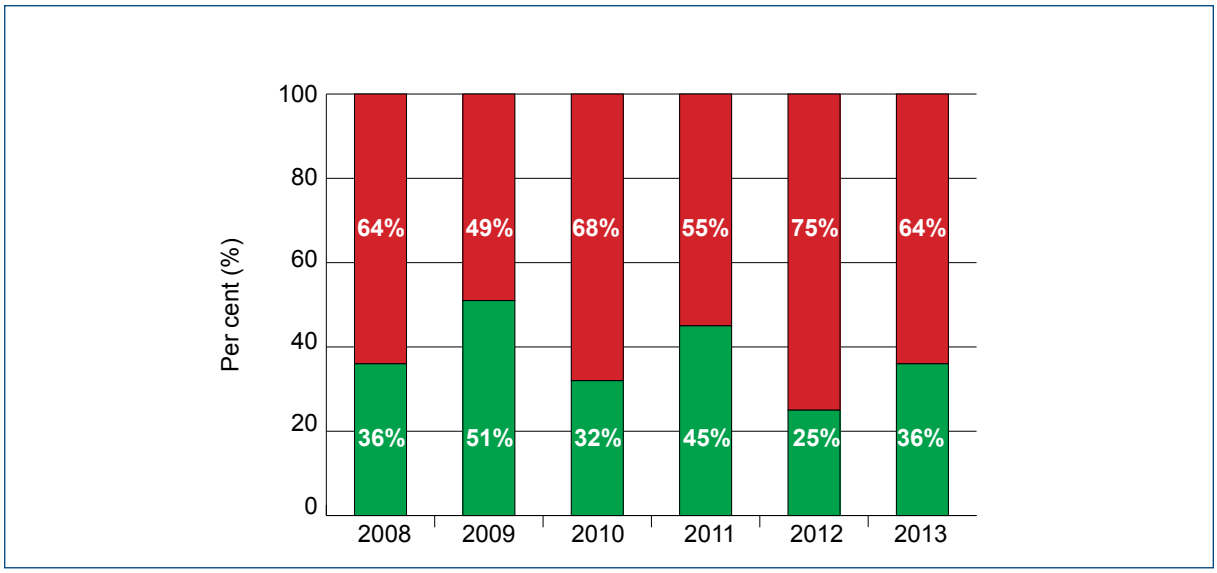

Figure 5: Business Continuity

Examples of findings

- a number of agencies did not have a BCP or if they did it was either in draft or had not been reviewed for a number of years
- while some agencies had extensive and detailed Disaster Recovery Plans (DRP) for systems and infrastructure, these plans had not been updated to reflect the current environment and had not been tested since their creation
- one DRP was last reviewed in 2006 and did not support the current IT environment
- many agency DRP's had never been tested or approved and in one case the DRP did not reflect their environment and referred to some infrastructure, key personnel and contacts that were no longer applicable.

Change control

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

There was no movement in change control practices from 2012 by agencies.

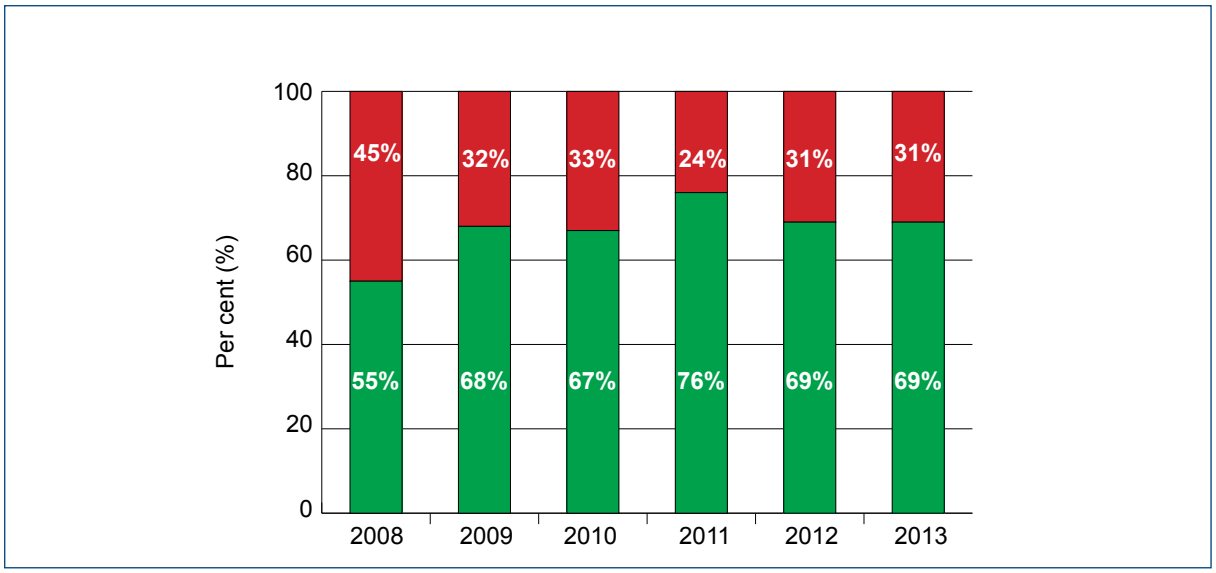

Figure 6: Change Control

Examples of findings:

- we found many agencies had no formal change management policies in place to ensure all changes to IT systems and applications are handled in a standardised manner
- one agency did not comply with their internal Change Management Policy, for record keeping and documentation. Records corresponding to major system changes could not be located. The current change control procedures were failing to reliably capture:
  - complete details of the change
  - who approved the change
  - implementation dates, times and duration
  - risks posed by the change, with evidence of adequate testing and back out contingency plans.

An overarching change control framework is essential to ensure a uniform standard change control process is followed, achieve better performance, reduce 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 an 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 an 11 per cent improvement from last year with 86 per cent of agencies now meeting our benchmark for management of physical security.

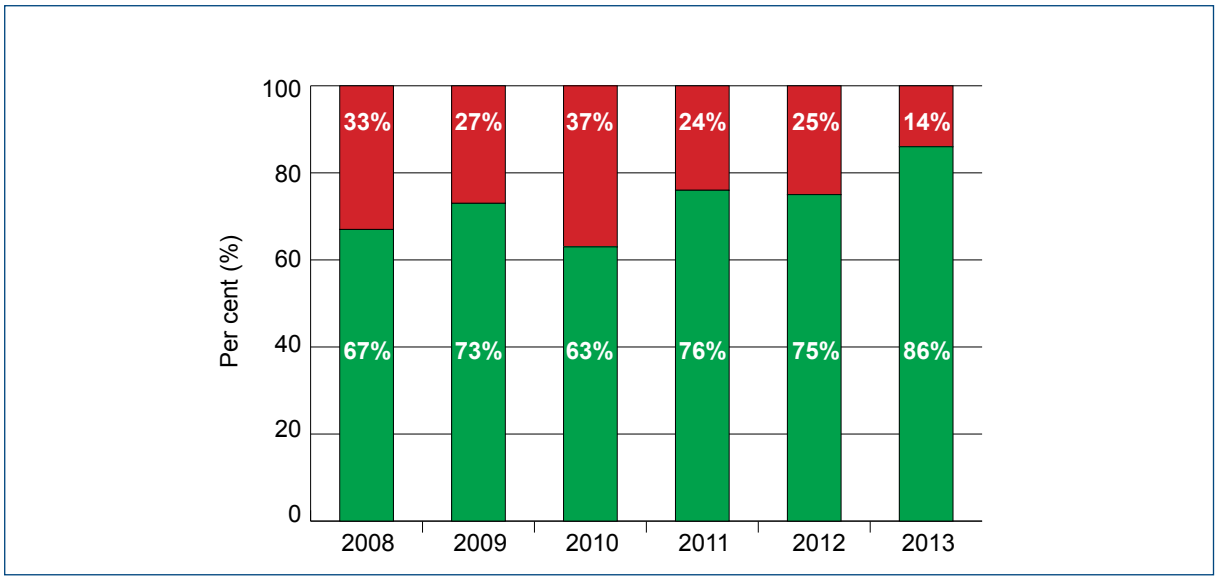

Figure 7: Physical Security

Examples of findings:

- a number of agencies could not provide reports on the maintenance and testing of the Uninterrupted Power Supply (UPS) and air conditioning
- power generators to be used in the event of power failure had not been tested.
- no fire suppression system installed within the server room
- a number of agencies where found not to have temperature or humidity monitoring configured to alert in the case of an event related to the server rooms
- some agencies continue to not appropriately restrict access to their computer rooms with staff, contractors and maintenance people having unauthorised access to server rooms. For example, approximately 150 people across one organisation have access to the computer rooms while the log detailing access to the computer room is not reviewed on a regular basis.

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

The majority of our findings require prompt action

Figure 8 provides a summary of the distribution of significance of our findings. It shows that the majority of our findings at agencies are rated as moderate. This means that the finding is of sufficient concern to warrant action being taken by the agency as soon as possible. However it should be noted that combinations of issues can leave agencies with serious exposure to risk.

The diagram on the next page represents the distribution of ratings for the findings in each area we reviewed.

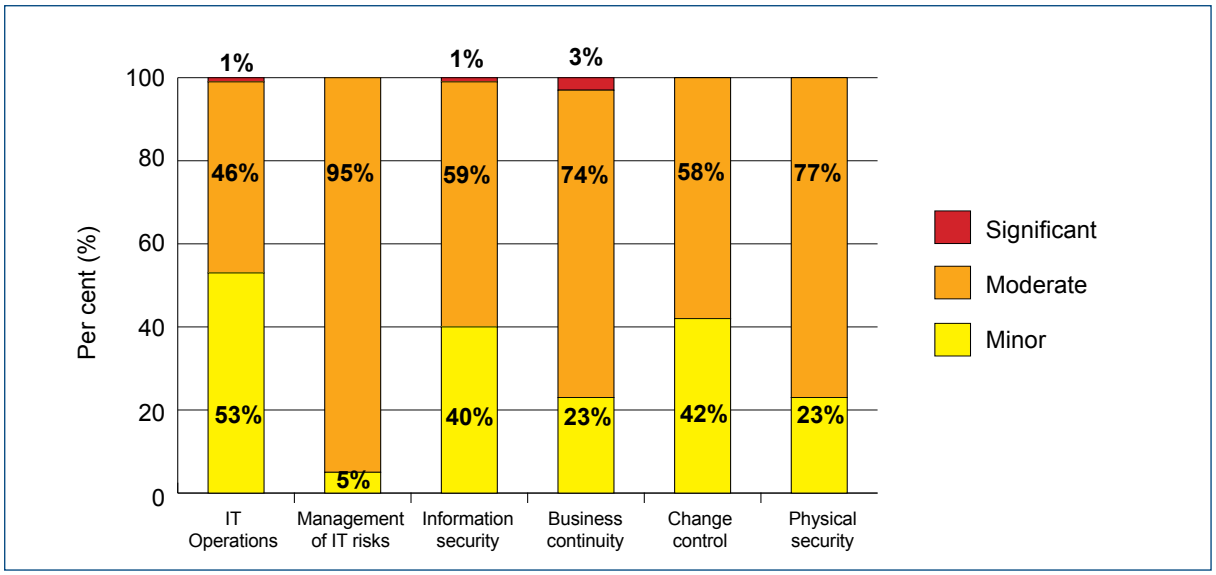

Figure 8: Distribution of ratings of findings across each area

Recommendations

Management of IT operations

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

Management of IT risks

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

Information security

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

Business continuity

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

Change control

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

Physical security

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

Auditor General's Reports

REPORT NUMBER	2014 REPORTS	DATE TABLED
13	Royalties for Regions - are benefits being realised?	25 June 2014
12	Government Funded Advertising	25 June 2014
11	Licensing and Regulation of Psychiatric Hostels	25 June 2014
10	Universal Child Health Checks Follow-Up	18 June 2014
9	Governance of Public Sector Boards	18 June 2014
8	Moving On: The Transition of Year 7 to Secondary School	14 May 2014
7	The Implementation and Initial Outcomes of the Suicide Prevention Strategy	7 May 2014
6	Audit Results Report – Annual 2013 Assurance Audits (Universities and state training providers – Other audits completed since 1 November 2013)	7 May 2014
5	Across Government Benchmarking Audits – Controls Over Purchasing Cards – Debtor Management – Timely Payment of Invoices	1 April 2014
4	Behaviour Management in Schools	19 March 2014
3	Opinion on ministerial decision not to provide information to Parliament about funding for some tourism events	18 March 2014
2	Charging Card Administration Fees	12 March 2014
1	Water Corporation: Management of Water Pipes	19 February 2014

Office of the Auditor General
Serving the Public Interest

Office of the Auditor General
Western Australia

7th Floor Albert Facey House
469 Wellington Street, Perth

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

T: 08 6557 7500

F: 08 6557 7600

E: info@audit.wa.gov.au

W: www.audit.wa.gov.au

Follow us on Twitter @OAG_WA

Download QR Code Scanner app and scan code to access more information about our Office