Records Management in the Public Sector
RECORDS MANAGEMENT IN THE PUBLIC SECTOR

This report has been prepared for submission to Parliament under the provisions of section 25 of the Auditor General Act 2006.

Performance audits are an integral part of the overall audit program. They seek to provide Parliament with assessments of the effectiveness and efficiency of public sector programs and activities, and identify opportunities for improved performance.

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
19 June 2013
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditor General's Overview</td>
<td>4</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>5</td>
</tr>
<tr>
<td>Overview</td>
<td>5</td>
</tr>
<tr>
<td>Conclusion</td>
<td>5</td>
</tr>
<tr>
<td>Key Findings</td>
<td>6</td>
</tr>
<tr>
<td>What Should Be Done?</td>
<td>7</td>
</tr>
<tr>
<td>Agency Responses</td>
<td>8</td>
</tr>
<tr>
<td>Background</td>
<td>9</td>
</tr>
<tr>
<td>What Did We Do?</td>
<td>11</td>
</tr>
<tr>
<td>What Did We Find?</td>
<td>12</td>
</tr>
<tr>
<td>All agencies have approved recordkeeping plans</td>
<td>12</td>
</tr>
<tr>
<td>Four agencies have key records outside their records management system</td>
<td>13</td>
</tr>
<tr>
<td>Testing found no evidence that agencies had not documented core business decision or activities</td>
<td>14</td>
</tr>
<tr>
<td>Agencies retain and store their records appropriately but may be incurring extra costs</td>
<td>16</td>
</tr>
<tr>
<td>Agencies need to improve the security of their records</td>
<td>18</td>
</tr>
<tr>
<td>Agencies could do more to encourage staff to maintain appropriate and complete records</td>
<td>20</td>
</tr>
</tbody>
</table>
Government agencies use public funds to provide services, deliver programs and manage assets. Good records support effective business practice and improve agency accountability and efficiency. As such, they are a cornerstone of organisational governance.

The importance of creating and managing records is enshrined in the *State Records Act 2000*. The Act emphasises the need for accountability and transparency in agencies’ recordkeeping practices. Unfortunately, too many of my audits identify poor recordkeeping practices with the consequent difficulty of tracking events and establishing facts through good evidence.

In addition to my role as Auditor General for Western Australia I am also the chairman of the State Records Commission. My experiences on the Commission have confirmed my understanding of the importance of good recordkeeping and the need for agencies to pay greater attention to this aspect of their business.

We have previously undertaken targeted audits of records management in 2004 and 2008. This audit examined records management at six agencies. It found some improvement though a range of weaknesses still remain. However, I was heartened by the prompt action of the agencies to acknowledge and address some of the issues identified.

This audit should be a reminder to all agencies to ensure that their records management systems are current and comprehensive, and that staff are trained and understand their responsibilities to maintain good records. For my part, I will continue to draw the Parliament’s attention to this issue.
Executive Summary

Overview

Good recordkeeping makes good business sense. It enables informed and consistent decision-making and provides evidence of key decisions and events. Recordkeeping is an important component of an agency’s governance framework that effectively supports the management of business activities and risks.

The *State Records Act 2000* governs agencies’ recordkeeping practices. The Act requires agencies develop a recordkeeping plan, and ensure records are created, retained or destroyed in line with this plan. Under the Act, the State Records Commission produces legally binding principles and standards to govern agencies’ recordkeeping. The State Records Office provides administrative assistance and technical advice to the Commission. It also advises agencies on recordkeeping, training, and developing recordkeeping plans.

This audit examined whether six agencies’ recordkeeping practices comply with the requirements of the *State Records Act 2000*. The audit reviewed records management systems and practice at:

- Bunbury Port Authority (BPA)
- Department of State Development (DSD)
- Fremantle Adult Mental Health Service, Fremantle Hospital (FH)
- Gold Corporation (GC)
- Midland Police Station (Police)
- Racing and Wagering WA (RWWA).

Conclusion

Although the *State Records Act 2000* has been in place for over a decade and all agencies now have recordkeeping plans, inadequate practices amongst the sampled agencies were still common. Most concerning is that key records are not being captured in some agency record’s management systems with the result that they can become lost or difficult to locate or be at greater risk of unauthorised access or alteration. Greater commitment to good recordkeeping systems on the part of some agencies would address the weaknesses we identified.
Key Findings

Records management systems

- All agencies met the key requirement of the State Records Act 2000 to have an approved recordkeeping plan, supported by policies and procedures. A recordkeeping plan identifies what is a ‘record’, and describes the process for ensuring that they are appropriately received, created, controlled, archived or destroyed.

- Four agencies had records that were not referenced in their recordkeeping plans. This makes it difficult for these agencies to manage these types of records. The most serious concern was the FH which uses a records management system to manage its patient records but has no similar system for corporate and non-patient records.

Documenting key decisions

- Despite the weaknesses identified above, we were able to track a sample of key business decisions or processes through each agency’s records. Documentation for these processes and decisions was relevant, understandable, sequential and supported the logic of the operational decisions made. We found no evidence of key records missing from our sample.

Ensuring adequate security over records

- Four agencies have assessed the risks associated with their records and developed business continuity plans to manage these. While Police has disaster recovery plans for its head office, these have not been provided to Midland or other local stations. There is also no specific risk management and business continuity planning for records held at Midland station. DSD does not have these plans in place but has recently drafted a disaster recovery plan for its records.

- Two agencies disposed of records after authorisation by senior officers and in compliance with their retention and disposal schedule. However, four agencies did not dispose of any records in 2012 and may be over-retaining records leading to higher storage costs.
All agencies use offsite storage facilities for some records. These records were stored securely. However, some agencies need to ensure these arrangements are reflected in their approved recordkeeping plan and use government approved suppliers for offsite storage.

BPA and DSD had not adequately secured access to their records management system by restricting the wide ranging administrator privileges to only a few staff. A person with unnecessary administrator access could inappropriately change or delete electronic records.

Training staff in records management

All agencies provide some training to their staff on records management, however only at BPA was it comprehensive and undertaken by all required staff. Adequate staff training is essential to ensuring that records are created and retained as needed.

What Should Be Done?

Agencies should ensure they manage their records well and meet the requirements of the *State Records Act 2000*. To do this, all agencies should:

- develop and maintain an up-to-date recordkeeping plan, supported by appropriate policies and procedures
- ensure records are listed in their records management system or other business information systems as set out in the agency recordkeeping plan and retention and disposal schedules
- ensure all business decisions are appropriately recorded
- ensure all records are securely stored and preserved for the appropriate length of time set out in the agency’s retention and disposal schedule
- document any off-site storage facilities in the recordkeeping plan
- adequately assess the risks to their records and have strategies in place to prevent or respond to any disasters or events affecting them
- ensure only appropriate access to the records management system is permitted
- ensure all staff with an operational need are adequately trained in records management.
Agency Responses

Bunbury Port Authority

The Bunbury Port Authority (BPA) agrees with the first six (6) key findings.

The BPA have now restricted administrator rights to key staff with operational needs only.

The BPA review of the Risk Management Plan in the records system indicated the document was included in the record system as a draft in December 2012, and as a final in April 2013.

The BPA are currently moving documentation from subsidiary drives to the record system, a process which will take three to six months to complete.

Department of Health

The Department of Health, on behalf of the state public health sector, accepts the findings and supports the recommendations made by the Auditor General.

Gold Corporation

Gold Corporation has found the audit of its Records Management by the Office of the Auditor General useful.

The significant finding that the (otherwise adequate) refinery records were not recorded on the Corporate TRIM records system resulted from the refinery being taken over on 1 April 2010 and the amount of work required to integrate its business in the rest of Gold Corporation. At the time of the audit, recording on TRIM was yet to be done. It will be completed by 31 March 2014.

There are four other moderate and minor findings and these will also be resolved, at the latest, by 31 March 2014.

The steps necessary to ensure an ongoing high level of compliance of Government’s requirements for Records Management are being put in place.
Good recordkeeping underpins agencies’ business activities and processes. It supports agency accountability, permits effective flow of information within and between agencies, and assists agency efficiency by ensuring information is readily identifiable and available. Each agency is responsible for managing its own records and ensuring they can be accessed when needed.

The *State Records Act 2000* (the Act) is the primary legislation governing agencies’ recordkeeping responsibilities. The Act requires agencies have a recordkeeping plan (RKP), identify their agency records, and ensure these records are received, created, controlled, archived or destroyed in line with the agency RKP.

Records may be in many formats, including paper, electronic, audio, and video. Most agency records are kept for seven to 10 years, but some need to be kept longer or permanently. The retention timeframes are set out in the agency’s approved retention and disposal schedule. Certain documents are designated as State archives and must be retained permanently.

Government records can be stored at a number of sites and for varying periods of time. For instance, an agency may store archive records permanently, at an offsite location managed by an external service provider.

All agency records need to be protected from theft; damage; and unauthorised destruction, access or alteration so they are available when needed. Adequate records also facilitate an agency’s response to freedom of information requests, and provide evidence to justify agency actions to an external audience, including reviews or any legal action.
Background

Under the Act, the State Records Commission (the Commission) produces legally binding principles and standards to govern recordkeeping by state agencies. These cover:

- government recordkeeping
- recordkeeping plans
- records appraisal
- restricted access archives
- compulsory transfer of archives
- outsourcing
- storage of State archives
- digital recordkeeping.

The Commission also supports the implementation and development of agency RKPs. The State Records Office of Western Australia (SRO) provides administrative assistance and technical advice to the Commission and is responsible for several functions including:

- providing records management and archival services to government agencies
- preserving archival records and making them accessible to the public and the community.

The SRO reviews and makes recommendations to the Commission to approve the agency RKP and its retention and disposal schedule. It has produced a template to help agencies develop or amend their RKPs. This includes areas for agencies to consider, such as contractors managing functions and services on behalf of government, increased use of electronic records, relevant government policy and industry standards, naming protocols, and risk assessments.

We last audited records management in 2008. Our key findings included:

- all agencies had approved plans and current policies
- records training programs needed improvement
- few agencies had adequate IT disaster management plans to protect their records management systems
- all agencies had inadequacies in the security of their electronic records systems.
What Did We Do?

The audit objective was to determine if six agencies’ recordkeeping practices comply with the requirements of the *State Records Act 2000*. In particular we asked whether agencies:

- have an up-to-date RKP and supporting policies and procedures
- implement all parts of their RKP in their management of documents for a sample of core business activities and decisions
- have recordkeeping systems that ensure adequate security (access and prevention of alteration or destruction) over physical and electronic records
- provide adequate records training to staff?

The audit reviewed records management at:

- Bunbury Port Authority (BPA)
- Department of State Development (DSD)
- Fremantle Adult Mental Health Service, Fremantle Hospital (FH). FH was audited as part of the Department of Health (Health).
- Gold Corporation (GC)
- Midland Police Station (Police)
- Racing and Wagering WA (RWWA).

During fieldwork we:

- examined agencies’ RKPs and other documentation
- audited a key business decision/process at each agency
- interviewed key agency staff
- sighted agencies’ records
- visited offsite storage facilities.

The audit was conducted in accordance with Australian Auditing and Assurance Standards.
All agencies have approved recordkeeping plans

All six agencies had approved RKP s that were prepared by experienced records officers, and approved by senior officers. Five agency plans were submitted to, and approved by, the Commission within the last five years. Health reviewed their RKP within five years as required under the Act and decided that they would amend the plan within a chosen time frame. We were advised a draft plan was submitted recently.

An RKP sets out how an agency will create, control, archive or destroy its records. It also assists with the naming and maintenance of records. When an agency develops an RKP it needs to consider the length of time records will be kept and where they will be stored. An RKP ensures an agency’s recordkeeping processes are appropriate, reduces the risk records are mismanaged, and the volume of records is controlled through timely destruction. Every government organisation must review their Plan within five years of its approval date and no extensions are provided to that requirement under the Act.

Fremantle Hospital operates under the Department of Health’s RKP. The Commission approved the current RKP in July 2004. It then reapproved this plan in March 2007 and required the Department completely review it by March 2012. Health subsequently advised the Commission it had reviewed the RKP and proposed to submit a revision by December 2012. Health then wrote to the Commission proposing that it submit the RKP by June 2013. We were advised during reporting that Health had submitted its draft RKP to the Commission on 29 May 2013.

Agencies support their RKPs with policies and procedures but three agencies’ policies need reviewing

All agencies had recordkeeping policies and procedures available on their staff intranet. However, some policies and procedures at DSD, Health and Police have not been reviewed for at least five years.

Recordkeeping policies and procedures provide operational detail to support the RKP. They identify what is a record, who can access it; and how it can be stored, transferred to different custodians, archived, preserved and destroyed. Their purpose is to help agency staff comply with their recordkeeping obligations.

DSD has not updated its recordkeeping principles and practices to reflect its creation as a separate department in 2009. The policies were originally prepared by the Department of Mines and Petroleum and refer to this agency’s systems, officers’ titles, mining plans and hours of business.
FH uses policies and procedures developed by the South Metropolitan Health Service (SMHS) to guide staff in their recordkeeping duties. These are up-to-date and are available for FH staff. FH also uses other records management policies and procedures produced by the Department of Health. While these are comprehensive, some policies have not been reviewed since 2004, including policies for non-patient records and IT service continuity for electronic records. Police have 19 sub-policies on records management of which 14 have not been reviewed for at least five years.

Four agencies have key records outside their records management system

All six agencies have electronic systems to manage their records. These systems identify records by title, location, creation date, author and custodian. However, we found four agencies had key records which were not listed in their records management system. Having records outside these systems makes it difficult to manage their existence, archiving and disposal in line with the agency RKP and retention and disposal schedules. Without a good record information system, an agency may not be aware that an important record exists or that it has been lost, stolen or destroyed. In addition:

- administrative effort can be wasted in creating a document that already exists or searching for it
- unmanaged records can be more easily accessed or altered without authorisation. For instance, staff, without an operational need, may access sensitive records.

The key records we identified as outside the sampled agency’s records management system were:

- FH’s non-patient records – these records cover all corporate matters such as business decisions, finance, planning, human resources and information technology. We were advised that Health uses electronic records management systems in some, but not all, operational areas and that the SMHS has contracted a consultant to address issues around non-compliance with the Act (this will include FH records).
- The GC’s refinery records – these detail the amount and grade of gold it has purchased and refined and allow the GC to reconcile and account for all gold received and processed. These records are currently stored on paper or electronically. The GC has advised these records will be migrated to, and kept in, the Corporation’s electronic recordkeeping system in line with its RKP.
What Did We Find?

- BPA’s risk management and business continuity plans — these detail how they will identify, assess, monitor and manage risks that may adversely impact on their operations. They are stored on subsidiary network drives and are not readily accessible by most staff who need to refer to them.

- DSD’s records relating to overseas business opportunities — DSD has six overseas offices which help West Australian businesses gain access to international markets for their products and services. The offices also promote investment opportunities in Western Australia overseas. They keep hardcopy records of their activities, for instance there are 100 files in one office. The records detail discussions with investors and developers, which have the potential to benefit the State and also local businesses.

Police has incident and investigation records stored in separate, dedicated databases, but not in its electronic records management system. The SRO advised that agencies are not required to register records in their records management system if they are already captured in a business information system. This is to avoid duplicating work.

The SRO also advised that the records contained in these systems must be included in the agency’s retention and disposal schedule, which is considered to form part of the agency RKP. The information system must be managed in line with agency policies, and procedures and its retention and disposal schedule. It may be appropriate to cross reference records relating to a particular business activity which are held in both systems but this would be determined by business need.

**Testing found no evidence that agencies had not documented core business decision or activities**

Good recordkeeping practices should be reflected in the completeness of records supporting core business activities or decisions. We looked at a core business decision or business process in each agency to determine the completeness of supporting records. Our testing found all agencies had documentation that was relevant, understandable, sequential and supported the logic of the operational decisions made. We found no indication of missing records in the following sample of business decisions:

- BPA lease agreement to establish a grain storage and handling facility (valued at approximately $30 million): This involved interaction with a large range of stakeholders including the public, local and state government agencies, legal experts, the media and various consultancy firms. The documents on file substantiated the proposal assessment, receipt of expert advice, stakeholder consultation and recorded the obligations of the parties in the agreement.
What Did We Find?

- State Agreement: DSD’s files recorded detailed discussions with government agencies, stakeholder groups, advice from consultants on important matters such as legal, environmental and indigenous issues, and negotiations and signing of agreements with other parties.

- Fremantle Hospital Patient Records: These records include details of a patient’s admission, medical history, diagnosis, medical test results, drug prescriptions and discharge details. The absence of any of these details could adversely compromise the health of a patient seeking future treatment at the Fremantle or other hospitals. The records audited included details on the patient’s medical assessment, treatment and discharge.

We also reviewed documents for FH’s accreditation. Although not listed in an electronic records management system, the file included key, relevant documentation of the process, decisions made and any follow-up action on issues raised during the inspection.

- Gold trading: The GC’s Treasury Depository records include client identification, deposit details, financial arrangements, transaction requests, confirmation of processed transactions and client requests to return deposited items or close trading accounts. The records audited supported the client’s identification and the processing and accounting of the client authorised transactions.

- Case investigation files – Midland Police Station: These record the initial complaint by a member of the public or an incident witnessed by a police officer on patrol. It also includes witness statements, victim statements, visits to and videos of the alleged crime scene, collection of evidence, video and audio interviews with suspects and witnesses, photographic or video or forensic evidence, review by a supervising officer, and a recommendation by the officer in charge to close the investigation or to have a prosecution brief prepared. These supported the decision to end an investigation with either no action required or for the preparation of a prosecution brief for charges to be laid.

- Racing Operations: RWWA’s records include grants made to racing clubs, and Racing Operations Integrity Assurance activities. The lack of these records could result in loss of client and community confidence. The RWWA records supported grant assessment processes and decisions, and payments to racing clubs. They also supported the initiation of investigations into the integrity or behaviour of trainers, jockeys and bookmakers.

Almost all BPA’s records are electronic. The other five agencies have a mix of electronic and paper-based records. Some agency records are in other media, such as video and audio.
Agencies retain and store their records appropriately but may be incurring extra costs

Four agencies may be over-retaining records and incurring added storage costs

Four agencies (DSD, FH, GC and RWWA) did not dispose of any records in 2012, although they had records which had reached the timeframe set for destruction. While agencies must protect and maintain their records in good condition, most records can be destroyed once they reach an age set out in the agency’s retention and disposal schedule. Both agencies that disposed of records did so in accordance with their RKP and retention and disposal schedules.

Physical and electronic records storage incurs a cost to the agency, particularly if these records are no longer needed and can be destroyed. Over-retaining records does however impact on costs as agencies pay more to the commercial providers of offsite storage.

Figure 1: Offsite records storage facility

Source: Recall
The increase in number and volume of records due to retention past the scheduled timeframe, and their subsequent offsite commercial storage, may escalate costs in future. If these are significant, it may be more cost effective to move towards digitising records sooner rather than later. But retention of digital records past the disposal date may also incur added costs. Agencies need to consider the ongoing costs, including storage of whichever format they store records in.

**Records, including archives, stored offsite are in a secure environment but some arrangements are not formalised**

We inspected offsite record storage facilities of all the agencies and found that they are physically secure. These facilities are provided by private companies and house both agency and State archive records. However, agencies do not always use the preferred government provider or document the storage of records offsite in their RKP.

All facilities we inspected have pest control, alarms with a continuous security service, fire detection and suppression systems and a back-up power supply. Staff must have police clearances. Because of the system of storage, staff know the client’s name but not the contents of the stored materials. Smoking is banned within the facilities and construction or repair work involving the use of heat is only undertaken after the required permits and supervision are in place. Electronic records are stored in air conditioned vaults and are only accessed by a small number of senior staff.

Agencies are required, under section 33 of the Act, to notify the SRO if they use off-site contractors to physically or electronically store their records and State archives. We were unable to evidence that Police or FH (through Health) had notified the SRO they used an off-site contractor to store some records.

All agencies, except GC, use a provider from the Common User Agreement (CUA) for offsite storage. The GC’s offsite storage provider for its gold refinery records is not on the CUA list. The refinery operated separately to the GC until 2010 and the arrangement is a legacy from that time. While it would be difficult and costly for these records to be shifted to another site at this time, the GC could approach the Department of Finance for approval to use a non-CUA provider.

SRO advised that, due to a lack of specialised storage space, it has been unable to accept the transfer of archives from government agencies as required under the Act since 2001. As a direct consequence, approximately 45 linear kilometres of identified State archives are stored within individual government agencies or alongside temporary records in commercial storage facilities. While these facilities do not meet the strict archival storage standards, they are accepted as an interim measure by the Commission. This situation also means that a wealth of archival information is generally inaccessible for research purposes, not only to government but also the community.
Agencies need to improve the security of their records

The Commission’s Standards require agencies protect their hard copy and electronic records against alteration and destruction. This can be done by limiting full administrator access to the recordkeeping system, having plans to manage risks and ensure business continuity if a disaster affects an agency’s recordkeeping system, and by regular audits of hard copy records to verify their existence and location.

Administrator access

BPA and DSD have allowed individuals without an operational need to have administrator access to the agency records management system. Administrator access includes high level privileges and the authority to make significant changes to records management systems and records.

An individual who has inappropriate administrator access could potentially make unauthorised deletions or changes to electronic records. In the case of hardcopy records, they could delete the record name from the system and take unauthorised custody of it. They could also change the status of a sensitive file and so allow inappropriate access.

The two examples of inappropriate administrator access we found were:

• two administrative assistants at BPA
• the names of two individuals who do not work for DSD or the system provider.
What Did We Find?

Risk management and business continuity planning

The Commission requires agencies ensure their records are protected and preserved. Paper records can be damaged by water or fire and electronic records can be deleted or altered if a system malfunctions. Agencies are less likely to prevent or respond to such events without adequate and up-to-date plans. Four agencies (BPA, FH, GC and RWWA) undertook adequate risk management and business continuity planning for their records management systems, including preparing disaster recovery plans.

These agencies have identified and assessed the risks and impacts of disasters on records and developed plans to mitigate the risks and respond quickly and appropriately to a disaster. The plans’ content and currency are regularly reviewed by these agencies’ audit, risk and executive committees.

DSD does not have a risk management plan but has drafted a disaster management plan and procedures for its records. A risk management plan is important to identifying particular risks that may compromise DSD’s ability to manage sensitive records such as negotiations for, and signing of, State Agreements.

Police does not have a business continuity plan for records at the Midland Police station. As well, the disaster recovery plan, produced by the Records Management Centre in Head Office, has not been disseminated to police stations. This makes it difficult for stations to respond effectively to any disaster impacting on their records held at the station, such as criminal investigations. Damage to these records could result in a prosecution being terminated due to a lack of evidence or officers having to regather evidence.

Records audits

Four of the six agencies do not audit hard copy records to ensure they physically exist and are under the control of the assigned custodian/owner. The SRO considers it best practice to conduct audits of high risk records to confirm their existence and location. DSD and RWWA audit agency records but do not report on the outcomes to management.

Records audits may show an increasing trend in the number of missing files over time. This may require corrective action, such as staff training. Regular reporting to senior management on audits undertaken increases their awareness of the state of the agency’s recordkeeping and may assist in supporting resource allocation to address specific issues.

FH does not have a records management system and so cannot audit to see if any corporate records are missing. However, FH inpatient records are tracked through its electronic records management system. As these files are tracked daily, FH does not audit these records.
What Did We Find?

**Agencies could do more to encourage staff to maintain appropriate and complete records**

All audited agencies provide some staff training on records management. This involves the use of relevant and understandable course content delivered by trainers with appropriate industry experience. However most training is ad hoc or could be improved. The Commission requires agencies to conduct a recordkeeping training program to ensure their employees comply with their RKP.

Training generally covers the importance of recordkeeping and how to create, archive, protect and destroy records. Insufficient or no training increases the risk that staff may mismanage records and breach the RKP and the retention and disposal schedule.

The Police train staff during induction on the use of its electronic records management system, but not recordkeeping principles generally. Further, they do not have an endorsed training strategy across the agency. However, the Police are developing a three tiered training program covering basic, intermediate and development training on records management. They propose to supplement this with a reporting framework to cover compliance, assessment and annual reviews of training content.

The GC and RWWA only have informal and ad-hoc training on records management. DSD’s training is comprehensive, but all three agencies do not test staff understanding and knowledge afterwards. BPA provides both comprehensive training and tests staff knowledge.

Health enrolls staff to receive records management training on the basis of operational need. However not all staff who have been enrolled for training have completed it (Figure 2).

<table>
<thead>
<tr>
<th>Area</th>
<th>Enrolled Staff</th>
<th>Enrolled Staff Trained</th>
<th>Percentage of Enrolled Staff Trained</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department of Health</td>
<td>22 184</td>
<td>13 453</td>
<td>61%</td>
</tr>
<tr>
<td>South Metropolitan Health Service</td>
<td>9 842</td>
<td>6 245</td>
<td>63%</td>
</tr>
<tr>
<td>Fremantle Hospital</td>
<td>2 968</td>
<td>1 691</td>
<td>57%</td>
</tr>
</tbody>
</table>

*Source: Health*

**Figure 2: Proportion of Health staff who have completed their assigned training**

The Public Sector Commissioner’s 2012 State of the Sector Report reported that most agencies (88 per cent) had partially or fully conducted recordkeeping training. While a high proportion of agencies are delivering training to some or all staff, there is still room for improvement across the sector.
# Auditor General’s Reports

<table>
<thead>
<tr>
<th>REPORT NUMBER</th>
<th>2013 REPORTS</th>
<th>DATE TABLED</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Delivering Western Australia’s Ambulance Services</td>
<td>12 June 2013</td>
</tr>
<tr>
<td>4</td>
<td>Audit Results Report - Annual Assurance Audits: Universities and state training providers and Other audits completed since 29 October 2012 – and Across Government Benchmarking Audits: Recording, custody and disposal of portable and attractive assets and Control of funds held for specific purposes</td>
<td>15 May 2013</td>
</tr>
<tr>
<td>3</td>
<td>Management of Injured Workers in the Public Sector</td>
<td>8 May 2013</td>
</tr>
<tr>
<td>2</td>
<td>Follow-on Performance Audit to ‘Room to Move: Improving the Cost Efficiency of Government Office Space’</td>
<td>17 April 2013</td>
</tr>
<tr>
<td>1</td>
<td>Management of the Rail Freight Network Lease: Twelve Years Down the Track</td>
<td>3 January 2013</td>
</tr>
</tbody>
</table>