

Report on  
CONTROLS, COMPLIANCE AND  
ACCOUNTABILITY AUDITS  
1997



Report No 7 - November 1997



A U D I T O R   G E N E R A L

---

*Western Australia*



# A U D I T O R   G E N E R A L

*Western Australia*

4th Floor Dumas House  
2 Havelock Street  
West Perth WA 6005

Telephone: (08) 9222 7500  
Facsimile: (08) 9322 5664

E-mail: [info@audit.wa.gov.au](mailto:info@audit.wa.gov.au)  
<http://www.audit.wa.gov.au/>

## VISION

of the

### Office of the Auditor General

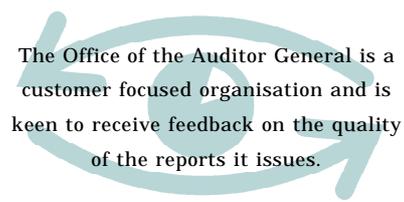
*Leading in Performance Auditing.*

## MISSION

of the

### Office of the Auditor General

*Through Performance Auditing enable the Auditor General  
to meet Parliament's need for independent and impartial  
strategic information regarding public sector  
accountability and performance.*



The Office of the Auditor General is a customer focused organisation and is keen to receive feedback on the quality of the reports it issues.

Report on  
CONTROLS, COMPLIANCE  
AND ACCOUNTABILITY  
AUDITS 1997

Report No 7 - November 1997



A U D I T O R   G E N E R A L

---

*Western Australia*



**AUDITOR GENERAL**  
***Western Australia***

**THE SPEAKER**  
**LEGISLATIVE ASSEMBLY**

**THE PRESIDENT**  
**LEGISLATIVE COUNCIL**

**REPORT ON CONTROLS, COMPLIANCE AND ACCOUNTABILITY AUDITS 1997**

This Report has been prepared consequent to audits conducted under section 80 of the *Financial Administration and Audit Act 1985* for submission to Parliament under the provisions of section 95 of the Act.

These audits evaluate aspects of public administration which impact on the control, accountability and performance of public sector agencies. They are concerned with improving the quality of public administration, assisting agencies in meeting their responsibilities and providing Parliament with assessments of public sector management in the areas covered by this Report.

Both specific agency audits as well as audits undertaken across a number of agencies are included in this Report. These latter audits are reported in a generic manner as the issues raised are based on findings from a number of agencies which are not necessarily attributable to one agency. Further information on the background to and reporting approach to these audits is outlined in the Introduction to this Report.

A handwritten signature in blue ink, appearing to read 'D D R Pearson'.

D D R PEARSON  
AUDITOR GENERAL  
November 12, 1997

# CONTENTS

<b>Introduction</b>	<b>1</b>
<b>Public Property Management</b>	<b>3</b>
Control and Custody of Public Property	4
Stores Management at Non-Teaching Hospitals	6
<b>Management of Information Technology Systems</b>	<b>9</b>
Privacy of Client Information	10
The 'Year 2000 Bug'	13
Control of Personal Computer Software	17
<b>Payroll and Personnel Management</b>	<b>21</b>
<b>Purchasing Goods and Services</b>	<b>24</b>
<b>Other Audits</b>	<b>29</b>
Industry Assistance	30
DOLA International — Overseas Projects	32
Ministerial Office Expenditure	35
Fines Enforcement Registry	37
Financial Controls at Autonomous Colleges	40
<b>Recent Reports</b>	<b>44</b>

## Risk Management in the Public Sector

Both public and private sector organisations, regardless of size, structure and type of operation, encounter risks from both external and internal sources. In the public sector, increased demands for accountability and the delivery of cost effective services, financial constraints, and changes to the role, structure and size of government agencies have increased existing risks and exposed agencies to new risks.

Managing and containing these risks is important as agencies' service delivery capability, the quality of their service and the extent to which they achieve their objectives can be adversely affected if risk exposures are not adequately addressed.

The *Financial Administration and Audit Act 1985* makes accountable officers and authorities responsible for the management of agencies' operational and financial performance. This is achieved through implementing appropriate internal control mechanisms to address identified risks and exposures. These internal controls should assist agencies to:

- operate efficiently and effectively to achieve objectives;
- report reliable financial and performance information; and
- comply with relevant laws and regulations.

## About this Report

In view of the importance of minimising risks and exposures, Controls, Compliance and Accountability (CCA) audits are conducted as part of the public sector audit mandate. These audits complement performance examinations of efficiency and effectiveness of public sector programs and activities and annual audits of agencies' financial statements and performance indicators.

CCA audits focus on financial administration and management effectiveness issues. Their objective is to contribute to improving agencies' operational performance, accountability, use of resources and compliance with legislation.

## Audit Themes

This Report contains a number of audits which are reported under the following themes:

- Public Property Management;
- Management of Information Technology Systems;
- Payroll and Personnel Management;
- Purchasing Goods and Services; and
- Other audits which include reviews covering new initiatives being undertaken by agencies and other issues of accountability.

---

## Introduction

A purpose of this Report is to alert and advise agencies not included in these particular audits of potential risks and exposures that they may be facing and have not adequately addressed. Agencies are advised to review their internal control systems to ensure that they adequately address all significant risks to which they are exposed.

## PUBLIC PROPERTY MANAGEMENT

Government agencies own or control a substantial portfolio of public property including computers, office equipment, furniture, motor vehicles and consumable stores with an estimated value of \$1.9 billion. A large proportion of this property is of low to medium value but includes items such as computer equipment which is portable, easily misplaced and attractive to theft.

Information such as the location, use and valuation of these assets is important in ensuring public property is protected from unauthorised use and loss and that financial reporting by agencies and the government is accurate.

In view of the importance of this area, two audits were undertaken across a number of agencies to examine:

- Control and Custody of Public Property; and
- Stores Management in Non-Teaching Hospitals.

# CONTROL AND CUSTODY OF PUBLIC PROPERTY

## Area of Concern

Assets (excluding consumable stores) controlled by public sector agencies which include vehicles, computer, office equipment and furniture have an estimated value of around \$1.7 billion. It is important that agencies have proper controls to safeguard these assets because they represent a large monetary investment. Complete and up to date records are also needed for accurate financial reporting.

The *Financial Administration and Audit Act 1985* and related Treasurer's Instructions detail how agencies should manage and maintain records and/or registers of public property. These Instructions require records to be kept for property with a value greater than \$1 000 but also allows for items with a lesser value to be recorded if necessary.

## What is the Potential Risk?

Many of these assets are highly portable increasing the risk that they may be stolen or used for unauthorised purposes. Adding to this problem is that only items with a value greater than \$1 000 are normally recorded for financial reporting purposes. Items under this value, including televisions, cameras and facsimile machines which are often portable and 'attractive', may not be recorded increasing the risk that any unauthorised use or loss of these items will go undetected.

## What Did We Do?

Audits were conducted at a sample of 12 agencies to assess whether agencies had identified risks relating to these portable and attractive assets and implemented appropriate management controls.

## What Did We Find?

The examination identified delays in recording asset purchases, lack of reconciliations, ineffective stocktake procedures and inadequate controls over asset disposals. Detailed findings included:

- agencies had not always addressed risks over attractive and portable assets and developed policies to provide guidance to staff. As a consequence, inconsistencies were noted over the types of assets being recorded with some attractive and portable assets with a value below \$1 000 not being recorded. Examples of these included cameras, overhead projectors, mobile phones and peripheral computer equipment;

- ten agencies were not recording acquisitions or disposals on a timely basis. Four agencies had a backlog of seven months of acquisitions, write offs and disposals awaiting entry onto registers. Testing of acquisitions during 1996–97 in four other agencies identified that between 19 and 44 per cent of their acquisitions had not been recorded at the time of the audit;
- ten agencies were not regularly reconciling asset registers to general ledgers;
- there was not always evidence that effective stocktakes of assets were undertaken as stocktake sheets were not always retained or were incomplete;
- evidence to show how stocktake discrepancies had been investigated and resolved was not always available;
- asset disposals made by nine agencies were not appropriately documented with details such as authority for disposal, how the asset was disposed of and disposal proceeds not always available; and
- instances where assets recorded as sold were still on hand and in use. These included laptop and desktop computers.

### What Does This Mean?

Inadequate records and controls over the location and use of assets means that:

- assets may be inappropriately used; and
- losses may not be detected either at all or too late to take effective action.

### What Should Be Done?

Public sector agencies should review the effectiveness of their internal controls over the custody of public property, particularly:

- identifying risks associated with the types of assets held by that agency and developing appropriate policies and procedures to ensure effective control;
- procedures for promptly recording all acquisitions and disposals;
- stocktaking procedures and the investigation of stocktake discrepancies; and
- the introduction of regular reconciliations between asset records and general ledgers.

## STORES MANAGEMENT AT NON-TEACHING HOSPITALS

### Area of Concern

Hospitals carry a wide range of different types of stores including consumables, building materials, stationery and pharmacy items. Inventory holdings at June 30, 1996 amounted to \$12.2m with expenditure on consumables, equipment, repairs and maintenance during 1995-96 totalling \$32.2m. After cash, stores are the type of asset most susceptible to theft. Given the type of expensive stock and potentially dangerous pharmaceutical products held in hospital stores it is essential that hospital management adequately supervise and control these items.

### What is the Potential Risk?

The main exposures associated with hospital stores are unauthorised use, undetected loss or theft, inaccurate recording, obsolescent stock, unnecessary holding costs, duplicate holdings and stock outs.

### What Did We Do?

The operations of eight non-teaching hospitals were examined to assess the adequacy of internal controls over general, pharmaceutical and engineering stores.

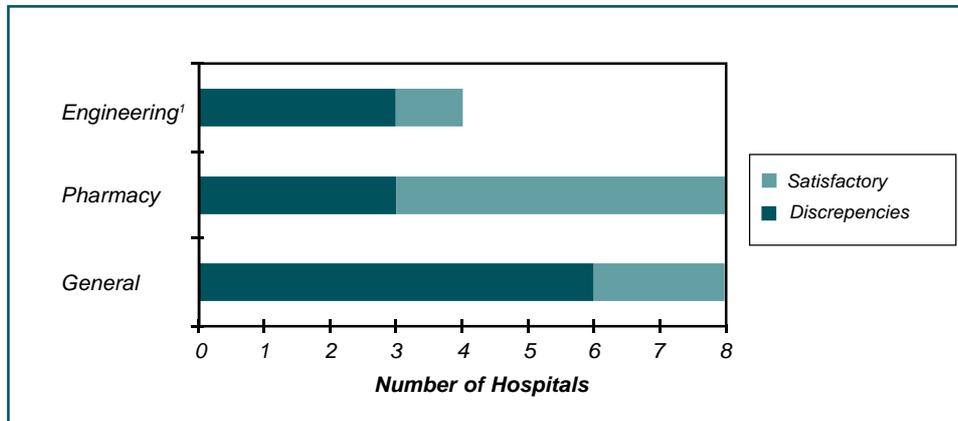
Work focused on key risk areas of supply management including inventory levels, acquisition and distribution of supplies and security over supplies held.

### What Did We Find?

#### Stock Recording and Monitoring

Over 60 per cent of inventories counted had discrepancies between stock on hand and stock records, with errors ranging from 15 to 50 per cent. In the majority of cases these discrepancies were attributed to a breakdown in controls over stock issues made out of hours.

A summary of errors noted is detailed in Figure 1.



**Figure 1:** Summary of supply areas with stock discrepancies

*Note<sup>1</sup> Only four of the eight hospitals held engineering stores*

Source: OAG

### Stores Purchases

In general, the hospitals examined had implemented adequate procedures over the ordering and acquisition of supplies particularly in relation to pharmaceutical and general supplies.

At two hospitals stock levels of engineering supplies were not based on usage trends or stock turnovers. In addition, reorder levels or economic order quantities had also not been established, making it difficult to determine whether appropriate inventory levels were being maintained.

### Slow Moving and Obsolete Stock

In the case of pharmaceutical stores and general stores generally effective controls to monitor slow moving items had been implemented.

However, two of the hospitals examined did not have formal procedures in place to identify slow moving or obsolete general stores.

Although not widespread, instances were also noted where general stores had reached their use by date and where new stores had been placed in front of old stores.

Engineering stores had the highest levels of slow moving items with 77 per cent of one hospital's engineering stores holdings with a value of \$18 000 having no movement over an eight month period.

### Stocktake Procedures

Unsatisfactory stocktake procedures were identified in 75 per cent of stores examined, with either :

- an absence of evidence of stocktakes being undertaken;
- incomplete follow-up of discrepancies identified during stocktake; or
- inappropriate allocation of stocktake responsibilities, with officers responsible for the purchase, receipt and issue of stores also conducting stocktakes.

### What Does This Mean?

The findings from this examination indicate that:

- recording of stores receipts and issues are unsatisfactory as illustrated by the high level of errors between physical stores on hand and stores records. This could result in store items being inappropriately used; and
- inappropriate inventory levels may be held for engineering stores as indicated by an absence of usage trends, known reorder levels and high levels of slow moving items.

### What Should Be Done?

Non-teaching hospitals should review their supply management practices to ensure that:

- reliable stocktaking procedures are used to periodically verify stock on hand to stock records;
- supplies received and distributed are accurately and completely recorded in a timely and efficient manner;
- appropriate inventory levels, based on economic re-order levels, are maintained; and
- obsolete inventory is promptly identified and disposed of.

# MANAGEMENT OF INFORMATION TECHNOLOGY SYSTEMS

The successful implementation and management of information technology (IT) systems is critical to the success of organisations. Public sector agencies, like most organisations, are making significant investments in implementing and managing IT systems to deliver services more efficiently and effectively and to manage resources.

Advances in technology are constantly changing how agencies use computers and this impacts on the risks and risk management techniques that management need to address. This section looks at the following issues which have a significant impact on government computing:

- privacy of client information;
- the 'Year 2000 Bug'; and
- control of personal computer software.

## PRIVACY OF CLIENT INFORMATION

### Area of Concern

Government agencies hold a large volume and range of information about members of the community which needs to be kept confidential. This includes police information, medical records and financial data.

In previous decades, computer files would contain only basic client details and a file number reference with personal details of clients being stored in secured filing cabinets which only a small number of people could access. Computing systems of the 1990's store and process enormous volumes of information and can make that information instantly available to many people. This improves efficiency but can have significant implications for privacy of client information.

### What is the Potential Risk?

Risks associated with agencies not keeping client information confidential and accurate are substantial. These include:

- agencies may not fulfil their responsibilities to clients. Unauthorised disclosure of personal information can cause loss of privacy, distress or potential losses to clients;
- clients may become reluctant to provide information that agencies need to perform their functions effectively; and
- information which can be altered may result in incorrect or ineffective management decisions being made.

### What Did We Do?

The review, conducted over the period September to April 1997, focused on the following two large computer systems that store client data and have different functions and security needs.

- The Department for Family and Children's Services introduced its Client and Community Services System (CCSS) in April 1994. CCSS supports the Department's core activities and is used daily by up to 600 staff in 62 sites across the State. The system maintains information on individuals who have contacts with the Department including information on reasons for contact, case management, services provided, financial details and other information that the Department collects.
- The Western Australian Department of Training has progressively implemented the College Management Information System (CMIS) in TAFE colleges throughout the State from 1995. This system supports the core activities of the colleges and stores information that

relates to members of the public who attend TAFE colleges. CMIS has four major functions, namely:

- ❑ college enrolments;
- ❑ curriculum management;
- ❑ student management; and
- ❑ assessment management.

## What Did We Find?

The two client management systems reviewed provided users with functionality supporting core activities. However, areas requiring attention include:

### Security Policies and Data Classification

Whilst there were relevant security procedures in place, neither department had an organisational security policy, approved by senior management, based on an analysis of its corporate data according to risk. This process is important in ensuring appropriate security controls are implemented which focus on securing information where the risk of exposure and potential extent of losses are greatest. These controls would include establishing which enquiries to sensitive information should be logged and reviewed.

This is a management task, rather than a technical computing task, and involves comprehensively analysing corporate data in whatever form it is stored.

### Managing Access to Computer Systems

The review identified that access to client data was not strictly limited to a need-to-know basis. Findings included:

- CCSS had facilities allowing two user managers to use powerful report writing software with unlimited and untraceable access to read, copy and change all client data;
- CMIS information technology staff could access and change system programs; and
- former staff and staff who had changed their position still had access to both these systems. A sample of 135 CCSS users identified four who did not have current employment status. In one area of the CMIS system there were a large number of staff with access to functions not required by their job.

### Data Integrity

When data is kept which is used to make decisions that impact on members of the public, there is a strong responsibility on agencies to ensure the data they use is complete and accurate. Instances were found in both systems where controls over data integrity were inadequate. For example:

- there were no checks by college management to ensure the accuracy of the calculation of a student's final subject result or the accuracy of the Statement of Academic Record;

# Management of Information Technology Systems

## Privacy of Client Information

- there was no documentation at the college level of key manual procedures that CMIS operators should perform to ensure the accuracy and completeness of data; and
- As a consequence of concerns about the accuracy of data in the CCSS, management implemented a process using computer programs to identify inaccuracies. Although these programs are useful for detecting obvious errors, they do not detect other less obvious errors, for example in case management history, which could occur due to lack of controls over data integrity. The Department advised that these computerised checks are supplemented by manual checking of records.

### Security Controls

To ensure the privacy of client data, agencies need to implement and maintain a series of security controls. Examples of security weakness were:

- passwords with access to highly confidential information not being changed regularly; and
- terminals left logged on and unattended.

### Action Taken

Management of these two departments have advised that all of the above issues have now been addressed.

### What Does This Mean?

The reliability, confidentiality and potential disclosure of sensitive information was at risk through agencies not developing and implementing appropriate controls to prevent:

- unauthorised and untraceable access and enquiries; and
- inaccurate information being held.

### What Should Be Done?

- Agencies that maintain client databases should classify that data according to privacy and confidentiality requirements and implement security procedures to provide the appropriate level of security.
- Access to client data should be managed on a strict need to know basis and should be terminated immediately when staff leave.
- Agencies should implement appropriate procedures to ensure the accuracy and completeness of client data.
- Security controls should be reviewed regularly to ensure that appropriate levels of security are maintained.

## THE 'YEAR 2000 BUG'

### Area of Concern

Potential problems arising from the 'Year 2000 Bug' have been well publicised in recent times. This problem results from computer systems storing and manipulating dates which use only two digits to denote the year. For decades this has worked well as whenever computers have referred to the year '00' it has always meant the year 1900. However, when the date changes from 99 to 00 in the Year 2000, many computer programs may interpret the year to be 1900 instead of 2000.

To raise awareness of this problem, the Premier wrote to all public sector agencies' Chief Executive Officers in May 1997 stating "While the root cause may be within computer systems, the resolution is a management issue ... Cabinet has agreed that effective action to manage this Year 2000 risk will be a consideration in CEO performance agreements."

### What Is the Potential Risk?

With less than two and a half years to go, agencies face the risk that:

- computer systems and the dependent agency operations may fail in the Year 2000; and
- the cost of correcting the 'Year 2000 Bug' is likely to be greater where management do not implement a structured risk based approach to resolve this issue.

The costs of correcting the problem are substantially unknown, however from available estimates, they are significant. For example:

- the Canadian Province of British Columbia estimated that expenditure of \$31 million would be required to limit exposures from the failure of government systems;
- Telstra Corporation estimated between \$30 million and \$100 million to modify or replace its systems; and
- the National Health Service in the United Kingdom estimated \$440 million to correct the problem.

### What Did We Do?

The audit, carried out in the period November 1996–March 1997, was conducted to assess the degree to which public sector management has addressed the risks associated with potential computer system failure caused by the Year 2000 problem. Eleven agencies were selected. In four agencies, the review was limited to evaluating the risk assessment, while in the other seven agencies the review also addressed the potential impact of system failures and the usefulness of available methodologies.

# Management of Information Technology Systems

The 'Year 2000 Bug'

## What Did We Find?

Table 1 summarises the audit findings.

Review Criteria	Inadequate Action Taken
Purchasing policies had been amended to require that new equipment and systems are Year 2000 compliant	9
Programming standards and policies had been amended to require Year 2000 compliance	9
Formal project structures and adequate corrective plans had been developed	9
Risk assessments included all key computer systems, including computer driven equipment	10
Risk assessments included applications developed by users and non IT professionals	11
Risk assessments included exposures to suppliers of critical goods and services	11

**Table 1:** Summary of audit findings

Source: OAG

Significant issues identified from these findings are:

### Awareness of the Problem

Generally senior management had an awareness of the 'Year 2000 Bug' but mostly understood the problem to relate to only financial and management information systems. This was the case with a major teaching hospital where previously unknown potential impacts of Year 2000 were identified by the audit. Management responded by initiating a review that found:

- the hospital's paging system could not handle the Year 2000. The paging system is used to contact medical staff in emergency situations. To operate correctly after 1999 the system needs to be completely replaced;
- the system used to control and monitor a wide range of plant and equipment including air-conditioning and power for the whole hospital did not correctly handle the Year 2000. Manual fall back procedures could be used but these would be costly and error prone if continued for an extended period;
- medical staff did not know whether critical medical and laboratory equipment could handle the Year 2000. Furthermore, they could not risk testing the equipment *in situ* as it could cause a critical failure; and
- there was no coordination between major hospitals to facilitate awareness and resolution of common problems. There was potential for duplication of effort.

The Health Department has now advised they have initiated a program to address the Year 2000 issues and coordinate their resolution across the public health sector.

In another agency a Year 2000 plan had concentrated on computer information systems. After the audit, management investigated further and found that the air-conditioning, PABX and building security systems were all connected to computers for monitoring and control, and none handled the Year 2000 correctly.

### Limiting the Risk

Most agencies audited believed that only older computers would be affected. Some agencies responding to a recent Public Sector Management Office survey indicated that they used new technology or standard mainstream packaged software and thus assessed their risks as minimal. This is not correct as was shown during the audit where several newer systems were found not to be Year 2000 compliant. For example:

- in one agency the Year 2000 was a major reason for replacing a computer system, however, the original specifications for the new system did not require Year 2000 compliance; and
- another agency had developed a system managing receipts from and payments to clients operating on new equipment. Although the system had only been operating for 12 months, the agency estimated that several months of programmer time were needed to make the system Year 2000 compliant.

### Corrective Action

With less than two and a half years until the Year 2000, comprehensive risk assessments and detailed corrective action plans are critical for agencies to effectively address Year 2000 compliance. The audit identified that nine of the 11 agencies had developed corrective action plans. However, of the plans developed several deficiencies were found, including:

- one agency had a draft project plan which allowed only ten weeks for correcting, testing and implementing changes. However, as the agency had not assessed all potential risk areas the time required was substantially underestimated.
- another agency had established a formal project and was using a commercial methodology to identify and evaluate risks. However, the assessment did not identify or evaluate all equipment reliant on computer processing.
- another agency identified 498 instances where programs required changes and scheduled ten months of programmer time to complete the task. However, as a project plan had not been developed there was no estimate of the time to test the programs and to plan and phase in the changes, leaving the risk that the project may not be completed before the Year 2000.

## What Does This Mean?

Failure to identify potential Year 2000 problems in all computerised systems and taking early steps to address these issues could result in the failure of critical systems and disruptions to government services.

## What Should Be Done?

- Agency management need to urgently assess all their activities to identify processes that rely on computer systems or computer operated equipment. This assessment should include all financial and management computer systems, all operational systems, all plant and equipment with computerised components and all suppliers or stakeholders that may supply critical goods or services.
- Purchasing criteria and programming standards should be amended to ensure all equipment purchased and software developed or purchased is Year 2000 compliant.
- Agency management need to develop corrective action plans that allocate responsibilities, prioritise corrective action and estimate resource requirements to meet the Year 2000 deadline.
- Coordination in specific areas should take place to facilitate awareness and timely resolution of common concerns and avoid unnecessary duplication of effort.

## CONTROL OF PERSONAL COMPUTER SOFTWARE

### Area of Concern

The increase in personal computing and technology has brought about greater exposures to the risk of installing illegal or unauthorised software and introducing computer viruses. Software can now be easily downloaded from the Internet and copied from one computer to another.

Concerns in this area were initially raised in the Auditor General's Second General Report of 1995 which identified that improvements were required in many agencies to:

- prevent illegal or unauthorised use of software; and
- reduce the risks posed by the introduction of computer viruses.

In March 1996, the Information Policy Council, which advises government on information and information technology (IT) issues, issued policy guidelines on Software Copyright Protection in the public sector. The policy states that:

- illegal or unauthorised software is not to be used; and
- unauthorised copying or distribution of software is prohibited.

These policy guidelines advise agencies to develop their own detailed policies and procedures on software copyright protection. The guidelines also explain the requirements of copyright and give practical assistance for managing software copyright.

### What is the Potential Risk?

The use of inappropriate software and computer viruses can have a significant impact on agencies operations, including:

- penalties of up to \$250 000 and civil damages for breaches of the *Copyright Act 1968*; and
- disruptions to services, loss of data, and waste of valuable IT resources if viruses or unstable and inappropriate software is installed.

### What Did We Do?

A follow-up of the issues raised in 1995 was conducted to assess the progress made. Twelve agencies were selected, six of which were included in the previous review. The following areas were examined:

- policies and procedures in place to control and monitor the use of software and prevent the introduction of computer viruses, including the maintenance of software registers and regular software checks; and
- provision of licences or other proof of ownership for software installed on computers.

### What Did We Find?

#### Software Policies

All of the agencies examined in this review had developed formal policies designed to control the use of computer software and reduce the risk of introducing computer viruses. This compares favourably with the 1995 results (Figure 2), indicating that agencies have recognised the need to develop policies and procedures on computer software. However, nine of the agencies reviewed had not addressed issues such as:

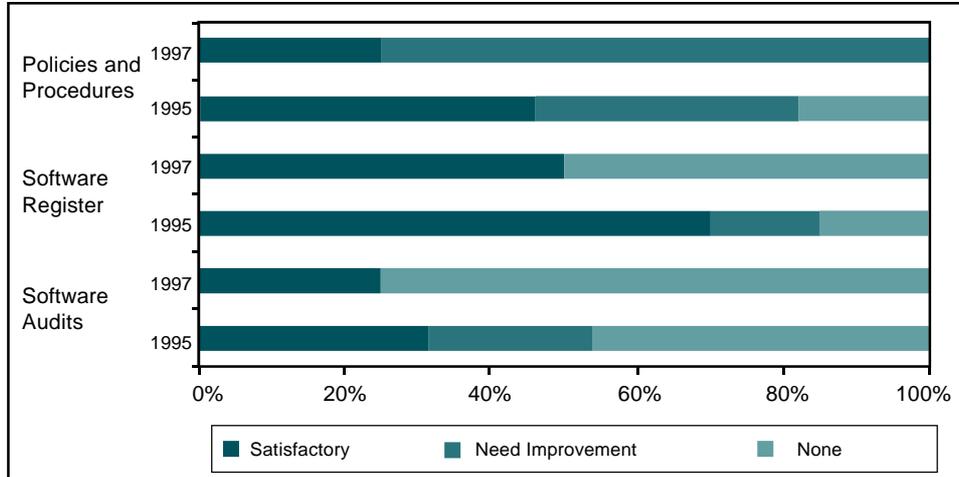
- the definition of illegal and unauthorised use of software and action to be taken when illegal software is found;
- the evaluation of non-standard software prior to installation;
- guidance to staff to reduce the risks posed by computer viruses; and
- the communication of policies and procedures to staff.

#### Computer Software Registers and Software Audits

Of the agencies subject to the follow-up review, six were not maintaining software registers which enable agencies to readily identify the software it is licensed to use and the location of that software. It was identified however that 'mainstream' products (such as Microsoft) were better controlled by agencies due to the introduction of software supplier agreements. These agreements required the supplier to maintain a register of purchases on behalf of the agency.

The lack of these registers also resulted in these six agencies being unable to conduct regular software audits. A further three agencies which were maintaining registers had not conducted software audits. The conduct of regular software audits to check the details of software installed on computers against software registers enables agencies to ensure that policies on software copyright protection are being complied with.

A comparison of results between the 1995 and 1997 examinations is shown in Figure 2 .



**Figure 2:** Agency controls over personal computer software: 1995 to 1997

Although all agencies examined in the follow-up review had developed formal policies to control computer software, fewer agencies than in 1995 had taken action such as maintaining software registers and conducting audits.

Source: OAG

### Proof of Software Ownership

An examination of software installed on computer equipment revealed that on average, almost every personal computer examined had one item of software for which proof of ownership could not be produced and/or unauthorised software existed (Table 2).

	1994-95	1996-97
Number of PCs examined	222	162
Number of items unauthorised or proof of ownership could not be located	24	129
Item/s per PC	0.1	0.8

**Table 2:** Prevalence of unauthorised software or software for which proof of ownership could not be produced

Source: OAG

The increase in potential illegal or unauthorised software compared with the 1995 review may be attributed to the overall absence of effective control procedures such as the maintenance of software registers and conduct of software audits. Factors relating to the greater use for personal computers have also increased the risk exposures from software copying, including:

- increasing access to the Internet by public sector agencies and therefore, ease in downloading or obtaining software which is not authorised; and

# Management of Information Technology Systems

## Control of Personal Computer Software

- increasing mobility of personal computers within agencies with new users inheriting software for which they cannot produce proof of ownership.

### What Does This Mean?

These findings show that the recording and monitoring of software used in agencies is inadequate. Consequently

- the potential public sector exposure to penalties arising from breaches of copyright is significant; and
- agency operations could be disrupted due to computer viruses.

### What Should Be Done?

Agencies should implement policies and effective procedures to control software installed on personal computers in line with the Software Copyright Protection Guidelines issued by the Information Policy Council in March 1996. These procedures should include:

- authorisation of software installation;
- maintenance of software registers; and
- regular software checks.

## Area of Concern

Human resources are a significant cost for most agencies. Recent data indicates that the Western Australian public sector employs approximately 96 000 people and pays almost \$4.1 billion in payroll related expenditure. The public sector has been subject to a number of significant changes in the human resources area in recent years including the decommissioning of centralised personnel and payroll systems, the use of external providers for payroll and personnel services, the introduction of workplace and enterprise bargaining agreements, and increased emphasis on productivity and efficiency with, in some cases, agency downsizing.

## What is the Potential Risk?

The changing human resource environment described above means that traditional internal controls over payroll and personnel systems may become inappropriate and less effective. Further, the introduction of new systems and industrial practices generally require new risk assessments and changed internal controls. If agencies do not address these factors they are exposed to increased risk of:

- inefficient human resource practices.
- incorrect or inappropriate payments to employees;
- incorrect interpretation of industrial award and agreement conditions; and
- inaccurate employee records.

## What Did We Do?

A sample of six agencies were selected where audits were conducted to assess the effectiveness of internal controls over human resource practices, including payroll and personnel systems. Payroll expenditure and staff numbers in these agencies were approximately \$152 million and 3700.

## What Did We Find?

### Higher Duties Allowance

Most of the agencies were making extensive use of higher duties allowance (HDA) which is a management tool to temporarily fill vacant positions or whilst employees are away on other duties or temporarily absent.

The percentage of employees receiving HDA during 1996 at the agencies examined ranged from 26 to 70 per cent. These findings indicate management of most agencies are not adequately reviewing and analysing HDA payments to determine their continued appropriateness.

Approximately 60 per cent of those on HDA were receiving this allowance on a continuous basis with no set finishing date. In addition, 30 per cent of staff had been receiving HDA for a period greater than six months. Cases were also identified where staff were receiving HDA to a substantially higher level. Examples included a Level 1 officer acting as a Level 7 and a Level 5 acting as a Level 9.

### Overtime

All of the agencies reviewed made use of overtime payments during 1996. The percentage of employees receiving overtime payments in individual agencies ranged from 32 to 58 per cent.

Reasons for using overtime included reductions in staff numbers and short term operational demands. However, there was no evidence in most agencies of any proper analysis of overtime payments to determine whether overtime was a cost effective resourcing strategy or alternatives such as time off in lieu or use of casual staff should be utilised.

### Leave Liabilities

Most of the agencies had not implemented strategies to address increasing leave liabilities. Examples of excessive accrued leave which is a liability that ultimately must be funded included:

- one employee with 25 weeks accrued annual leave;
- three employees with more than 18 weeks accrued annual leave; and
- three employees with 26 weeks accrued long service leave.

### Employee Records

In three of the agencies' employee records were inadequate to support various payroll related payments. For example:

- audit experienced difficulties in verifying the accuracy of some allowance and long service leave payments as documentation supporting these payments was not fully completed or could not be located; and
- sixty per cent of overtime claim forms examined in one agency did not describe the reasons for the overtime worked.

In three of the agencies security over personnel records was also unsatisfactory with access to the personnel area not always secured or restricted to authorised employees.

### Policies and Procedures

Two agencies had not developed and documented their human resource policies and procedures including the key areas of recruitment, terminations and equal employment opportunity to provide guidance to staff and assist in ensuring consistent and appropriate practices are followed.

### What Does It Mean?

Agencies are not adequately monitoring and reviewing payroll and personnel practices and associated risks. Consequently they may:

- make unnecessary or incorrect HDA, overtime, allowances or leave payments;
- face difficulties in funding accrued leave liabilities;
- not comply with industrial awards and agreements, and legislation; and
- lose sensitive employee information.

### What Should Be Done?

Agencies should:

- review the effectiveness of existing HDA and overtime practices;
- adopt strategies to manage leave liabilities;
- develop and document comprehensive human resources policies and procedures;
- ensure payments are adequately documented; and
- restrict access to personnel records to authorised employees.

# PURCHASING GOODS AND SERVICES

## Area of Concern

Government purchasing of goods and services in Western Australia amounts to approximately \$2 billion each year. There has been increased delegation of purchasing responsibilities to individual agencies by the State Supply Commission (SSC) in recent times. However, both within and outside of individual agencies' delegated limits there exists a policy framework that is to be observed.

This policy framework is designed to ensure all purchasing is conducted in an efficient and effective manner and that the best interests of the State are always considered. There is an expectation by suppliers and the public that all government purchasing is open and honest and achieving the best value for money.

## What is the Potential Risk?

The major risk agencies face when purchasing is that they may not be achieving value for money. Further, deviation from SSC supply policies can adversely impact the probity of purchasing arrangements.

## What Did We Do?

A sample of 12 agencies, including eight non-teaching hospitals, with delegated purchasing responsibilities were examined to assess their purchasing practices and degree of compliance with SSC supply policies. The audit focused on purchases of goods and services and did not include areas such as capital works purchases and contract management issues.

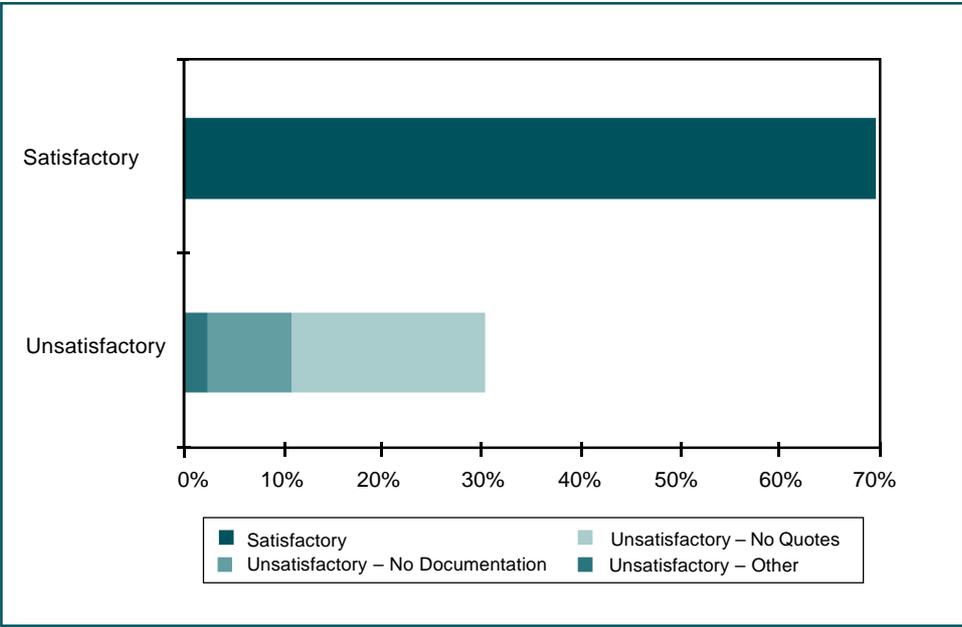
## What Did We Find?

Although the procurement functions of the agencies examined were generally well controlled, the following value for money and compliance matters were identified which need to be addressed to further enhance the effectiveness of the purchasing function.

### Quotation Procedures

To ensure fair, open and sufficient competition SSC supply policies require verbal quotes for purchases below \$5 000 and written quotes for purchases between \$5 000 and \$50 000. Purchases over \$50 000 are required to go to formal public tender.

Testing of purchases below \$50 000 showed verbal and written quote procedures were not followed in 30 per cent of the purchases examined. Documentation could often not be provided to show that quotes had been obtained in regard to the expenditure of public funds (refer Figure 3).



**Figure 3** : Summary of testing verbal and written quote procedures

Source: OAG

For purchases over \$50 000, tender documentation was of a high standard and tender procedures were correctly applied.

**Regional Purchasing Policy and Quotation Procedures**

Agency misunderstanding of the regional purchasing policy also contributed to quotation procedures not being followed. This policy is a strategy to support country areas and to promote economic development across the State. It is mandatory for all government agencies and provides the authority for them to purchase locally goods and services up to the value of \$5 000. Quotation procedures must still be complied with, however a loading is allowed for local suppliers in some circumstances.

This examination identified a degree of confusion at country agencies over the application of this policy. In most country agencies, quotations were not always being sought because of the mistaken belief that they are not required under the policy.

**Effective Competition**

Increased competition for government purchasing provides greater assurance that the best value for money is achieved.

## Purchasing Goods and Services

The review of purchases of goods and services below \$50 000 (where tendering procedures are not required) revealed that 20 per cent of purchases were made without competition being sought and a further 10 per cent of purchases made had insufficient evidence to indicate that competition had been sought. Examples of such purchases include:

<b>Good/Service Purchased</b>	<b>Amount \$</b>	<b>Comment</b>
Painting Services	10 784	Quotes were not obtained
Marketing Services	25 000	Quotes were not obtained
I.T. Equipment	22 800	Only 1 quote obtained
Consultancy Service	15 000	Quotes were not obtained

Instances were also noted where agencies were routinely purchasing from previous suppliers without testing the market on a regular basis to ensure they continue to obtain the best price.

### Alternative Purchasing Options

Panel contracts and standing orders are a few of the many arrangements that can be entered into by agencies for the procurement of goods and services. Under these arrangements, firms are selected as the nominated supplier of like items or services for a period of time. This results in agencies saving time and costs as separate tendering or quotation procedures do not have to be undertaken. They can also increase an agency's purchasing power and its ability to negotiate prices.

The audit found that little attention is being given by agencies to investigating these alternative purchasing methods. In some cases, agencies were purchasing quantities of like goods and services over an extended period of time with each purchase viewed as a separate transaction. In some cases when viewed on an annual basis these items and services represented significant dollar amounts.

#### **CASE STUDY No 1**

One agency placed an initial order for uniforms amounting to \$41 000. The agency would need to place subsequent orders both during the year and into the following year. However, the initial order and each subsequent order were viewed by the agency as individual purchases. Alternative purchasing arrangements, for example period contracts, had not been considered by the agency and could have resulted in savings on these purchases.

These alternative approaches to purchasing also overcome a problem faced by a number of agencies in regional areas, where suppliers do not respond to requests for quotations generally because they had not been successful in the past. In these situations, agencies should consider entering into arrangements for panel contracts or standing orders with the preferred suppliers. Benefits of these type of arrangements also include the reduction in time and effort involved in obtaining individual quotes.

### Purchase of Goods and Services on Corporate Cards

The audit identified that many agencies are not gaining the full benefits of corporate credit card facilities which have a lower processing cost than normal payment arrangements which require separate cheques to be issued for each purchase. Only one of the agencies examined encouraged the use of corporate credit cards for all purchases below \$1 000. In other agencies corporate credit card usage was restricted to senior executive officers only who are not involved with purchasing activities.

### Local Purchase Orders

Local purchase orders (LPOs) are a manual purchase order originally designed for emergency or one-off purchases. LPOs have higher processing costs as these documents must be matched with invoices and separate cheques issued. These costs result in LPOs not being as cost effective a purchasing mechanism, especially for low value items.

The audit identified a high usage rate of LPOs across most agencies, including several hospitals. The use of LPOs in these circumstances was not warranted as alternative purchasing mechanisms were available.

#### CASE STUDY No 2

One agency examined used LPOs extensively for low dollar value purchases. On receipt of the supplier's invoice the details of the purchase were then entered into the computerised purchasing system to generate a system purchase order number to allow for payment processing.

This resulted in a manual purchase order as well as a computer generated purchase order being raised for purchases made, effectively duplicating work and increasing overall account processing costs.

### What Does This Mean?

The combination of a lack of competitive quotes, poor documentation to support that quotes had been obtained, and non-compliance with SSC policies significantly increase the risk that individual government agencies and the State are not achieving value for money. Additionally agencies are unable to adequately demonstrate proper accountability in the expenditure of public funds.

### What Should Be Done?

Accountable officers and authorities should:

- ensure that staff with purchasing responsibilities fully understand SSC supply policies and guidelines;
- identify and adopt opportunities to improve the efficiency and value for money of purchases of goods and services; and
- retain evidence which demonstrates their compliance with Government purchasing policies and guidelines and adoption of competitive purchasing practices.

## OTHER AUDITS

This section contains a series of audits covering initiatives implemented by agencies and other identified issues. These examinations are:

■ **Department of Commerce and Trade: Industry Assistance Funding Investigation**

Complaints alleging collusion, price fixing and fraudulent claims in relation to this program were made in 1996. A review of the investigation of the allegations by the Department was undertaken to provide assurance that the complaints had been adequately investigated.

■ **DOLA International**

This examination reviewed aspects of the operation of DOLA International which was established in 1991 to export Western Australian expertise in land management.

■ **Ministerial Office Expenditure**

A review of expenditure and accounting records maintained for Ministerial Offices was undertaken to assure appropriate accountability requirements were met.

■ **Fines Enforcement Registry**

The *Fines, Penalties and Infringement Notices Enforcement Act* came into operation in 1995. It was established with the intention of increasing the proportion of infringement notices and fines paid so as to reduce costly enforcement actions and imprisonment rates. This examination reviewed the procedures and practices established to implement the requirements of the legislation.

■ **Financial Controls at Autonomous Colleges**

As from January 1, 1997, 11 colleges were created as separate statutory authorities autonomous from the Western Australian Department of Training. A review of the financial controls at a sample of colleges was undertaken to identify significant areas of concern prior to these colleges reporting for the initial period of operations.

## INDUSTRY ASSISTANCE

### Area of Concern

In October 1996, a complaint was made to a member of Parliament about the National Industry Extension Services (NIES) Program operated by the Department of Commerce and Trade (the Department). This followed an earlier complaint received by the Department in July 1996 relating to fraudulent claims. These allegations included:

- collusion and price fixing practices in the use of consultants involving Departmental staff and some consultants; and
- fraudulent claim for funds being made by a company for consulting services which were not provided.

The NIES Program is a cooperative venture of the Commonwealth and State Governments to assist manufacturing and service companies improve their international competitiveness. Client managers from the Department are available to companies to help diagnose problems and assist with access to relevant services under the Program. Where the services of expert consultants were required, the client managers provided a list of suitably accredited consultants from which companies were able to make a selection. For major services, a company must have obtained competitive quotations from at least two consultants.

Once the services have been provided by the selected consultant and paid for by the company, the Department then provided a contribution (normally 50 per cent but may be up to 75 per cent) by way of recoupment to the company upon evidence of payment and satisfactory service completion.

### What is the Potential Risk?

These types of allegations, if not properly resolved, adversely affect the agencies operations and the credibility of individuals concerned.

### What Did We Do?

In view of the serious nature of the allegations, it was decided to review the investigation of the allegations by the Department to provide assurance that the complaints had been adequately investigated and matters arising pursued to finality.

## What Did We Find?

### Collusion and Price-Fixing Allegations

The Department commissioned its internal auditors in November 1996 to conduct an audit of departmental records to determine whether there was substance to the allegations. The findings of the internal auditors were inconclusive.

This Office's subsequent review concluded that further lines of inquiry were necessary so a more definitive outcome could be reached. This approach was agreed to by the Department. In consequence, a larger sample of records were tested and interviews with some departmental managers and recipients of assistance were conducted.

Following this additional work it was concluded that the allegations of collusion or price fixing were not sustainable.

### Fraudulent Claims

The Department's internal audit identified that amounts claimed by a client company were not supported by adequate file documentation, nor was there evidence that accounts submitted for reimbursement had been paid by the client. In addition, an instance of 'double dipping' of departmental funds and attendance at NIES courses by non-client employees were identified.

It is acknowledged by the Department that a failure to perform proper checks of some supporting documentation may have allowed the client to be improperly recouped. Improved procedures have been implemented to ensure that payments are made in accordance with Departmental policies and procedures, and are supported by adequate documentation.

## What Does This Mean?

The Department has pursued all reasonable lines of inquiry in relation to these allegations and taken action to address the shortcomings identified.

## What Should Be Done?

The Department should continue to implement improved control procedures which appropriately deal with the risks involved in managing funding programs.

## DOLA INTERNATIONAL — OVERSEAS PROJECTS

### Area of Concern

The Department of Land Administration (DOLA) established DOLA International in May 1992 to participate in the development of a land management system in Vietnam. Based on DOLA's submission, Cabinet in 1996 approved an extension of the Program to June 30, 1999, with a target of self sustainability within that time frame.

International operations by government agencies result in different risks not normally associated with traditional government activities.

### What is the Potential Risk?

In exporting government services to developing countries, issues which need to be addressed include:

- establishing suitable contractual arrangements;
- protection of assets; and
- ensuring payment arrangements are satisfactory including managing currency fluctuations.

### What Did We Do?

A review was conducted to determine:

- how DOLA International addresses the risk exposures;
- the adequacy of measurement and reporting systems in place to monitor progress towards achievement of self sustainability by June 30, 1999; and
- whether DOLA International was operating within the terms of its objective.

To facilitate an assessment of self sustainability, estimates of profitability were developed based on:

- past achievements;
- projections supplied by DOLA International on the probability of winning future projects;
- overheads applied on the basis of activity; and
- the prospect of winning larger projects as DOLA International gains greater international experience and market credibility.

## What Did We Find?

### Management of Risks

DOLA International has implemented effective strategies to manage risks identified with overseas projects in developing countries. These are shown below:

Risk	Strategy
<i>Buyer Insolvency</i>	DOLA deals only with reputable aid agencies funded through government aid programs.
<i>Delays in payments</i>	Payments are made directly by the aid agency, rather than by the developing country, in accordance with contract milestones.
<i>Repudiation of Contract</i>	The contract is with a reputable aid agency.
<i>Currency Fluctuations</i>	Where possible all transactions are in Australian Dollars.
<i>Professional Error</i>	DOLA requires its contractors to take out professional indemnity insurance.
<i>Imposition of controls on repatriation of profits</i>	Payments are made directly by the aid agency, rather than by the developing country.
<i>Expropriation</i>	DOLA does not own assets in foreign countries.
<i>Property loss resulting from war or civil disturbances</i>	DOLA does not own property in foreign countries. There is also redress under contracts for delays caused by civil disturbances.
<i>Workers Compensation</i>	DOLA has negotiated a special workers compensation package to cover all staff working overseas.

**Table 3:** Risks associated with exporting government services to developing countries and the action taken by DOLA to address those risks.

Source: OAG

### Meeting Objectives

The objective of DOLA International is to “export land administration expertise ... to provide financial benefits for Western Australia”. DOLA International is operating within the terms of this objective. In the five years to June 30, 1996 DOLA International had won or participated in 11 projects valued at \$10.5 million and had provided over \$500 000 of consultancy work to the private sector. Although performance targets are set for each project, overall performance indicators were not reported to demonstrate the extent to which the program objective was being achieved.

### Self Sustainability/Profitability

The assessment of future profitability indicates that the DOLA International program is on target to achieve self sustainability by June 30, 1999. The examination identified the following issues which need to be addressed to improve the monitoring and reporting on international activities:

- whilst detailed and accurate financial records for each of the 11 projects were maintained, there were no financial reports to determine the overall profitability of the program for any period of time;
- there was no revenue recognition accounting policy in place for international projects. Revenue was accounted for only when payments were received (that is on a cash basis). To be able to determine profit, revenue should be recognised over the life of the project rather than at the end;
- consistent with cost allocation methods applied by DOLA for its domestic Programs, overheads were being allocated to DOLA International based on overall staffing numbers. This resulted in the costs of DOLA International being overstated.

### What Does This Mean?

There is the possibility that:

- unless an accounting policy is developed to recognise project revenue on an accrual basis it will not be possible to accurately measure self sustainability for a period of time;
- the cost of operating the international program have been overstated; and
- without published performance indicators independent assessment of achievement by DOLA International against its Program objective is not possible.

### What Should Be Done?

To assure effective assessment of self sustainability DOLA should:

- develop accounting policies and records which will facilitate improved measurement of DOLA International's profitability;
- review the method of allocating overheads to more accurately reflect the cost of operating DOLA International. Consideration should be given to allocating overhead on an activity basis rather than on overall staffing numbers; and
- develop key performance indicators of the efficiency and effectiveness of DOLA International.

## MINISTERIAL OFFICE EXPENDITURE

### Area of Concern

Minister's offices, which are attached to host agencies, are responsible for expenditure associated with undertaking the duties of Minister's portfolios. Expenditure for the 17 Ministerial Offices in 1996–97 is around \$7.5 million, excluding salary and some other costs such as office rent which are paid by the Ministry of Premier and Cabinet (the Ministry).

### What is the Potential Risk?

Public sector expenditures are subject to the requirements of the *Financial Administration and Audit Act 1985* which are supplemented by guidelines contained in Circulars to Minister issued by the Premier, including:

- Guidelines for the Use of Credit Cards and Taxis in Ministerial Offices; and
- Guidelines for Expenditure on Official Hospitality.

As Ministerial Offices often employ staff from outside the public sector, the risk of payments being made which do not follow these requirements could be increased due to a lack of awareness and knowledge.

### What Did We Do?

Four of the 17 Ministerial Offices were examined for procedures and controls in place from July 1, 1996 to March 31, 1997 for:

- authorising and processing expenditure; and
- purchasing and recording assets.

The audit did not include expenditures based on entitlements determined by the:

- Salaries and Allowances Tribunal such as salaries, electorate allowances, motor vehicle allowances, and travelling allowances (paid by the Legislature); and
- Treasurer such as electorate air travel (including spouse and dependant travel), parliamentary electorate offices and Imprest Scheme (paid by the Ministry).

#### What Did We Find?

The audit found that the controls and procedures implemented by Ministerial Offices were generally satisfactory. Exceptions were noted in the following areas:

- corporate credit card, hospitality and taxi cabcharge payments were not always being made in accordance with the relevant guidelines. Examples included supports and certifications not being provided for corporate card payments and details of attendees and the purpose of hospitality payments not being recorded. Officers approving these payments had also not ensured that proper certifications and supports were provided; and
- records of assets purchased for Ministerial Offices were not being adequately maintained by host agencies.

#### What Does This Mean?

The lack of certification and supports made it difficult to confirm whether payments were for official purposes, while the lack of asset records increases the risk that assets may be removed or lost.

#### Action Taken

From July 1, 1997, the Ministry assumed responsibility for the processing of all Ministerial Office expenditure.

To ensure that relevant staff in Ministerial Offices are aware of the financial administration requirements relating to Ministerial Office expenditure, the Ministry has:

- issued a procedures manual to each Ministerial Office. In addition, a seminar was held for Chiefs of Staff and Executive Officers which provided guidance and clarification on public sector financial administration requirements; and
- conducted a complete stocktake of assets at each Minister's Office. Assets valued at \$1 000 or more have been included on the Ministry's asset register.

## FINES ENFORCEMENT REGISTRY

### Area of Concern

The *Fines, Penalties and Infringement Notices Act 1994* came into operation on January 1, 1995 and is administered by the Ministry of Justice (the Ministry). The main purpose of the Act is to increase the proportion of court fines and infringement notices paid and to reduce the number of costly enforcement actions and number of persons imprisoned for non-payment. The Act also establishes the Fines Enforcement Registry (FER) and the position of Registrar.

The Act provides that Court of Petty Sessions fines not paid within 28 days may be registered with the FER for enforcement. Similarly, unpaid traffic and other infringement penalties may also be referred to the FER 28 days after issuing a final demand.

In respect to court fines, there are several enforcement options available to the Registrar. Driver or vehicle licence suspension is the first option. The Act also provides the Registrar with the option to issue a warrant of execution to the Sheriff for the seizure of goods in order to satisfy outstanding debts. If the action is not satisfied in this manner, work development orders may be issued and if the court fine is still not satisfied warrants of commitment may be issued for the offenders arrest and imprisonment.

In respect to infringement notices, the Registrar initially provides the option for offenders to pay the penalties in full or elect to have the matter determined by a Court of Petty Sessions. If the offender does not adopt either of the above options the only available enforcement action for the Registrar is the suspension of the offenders driver or vehicle licence. The Act does not provide for any further recovery action by the Registrar, although there is provision for the alleged offender or the prosecuting authority to take the matter to Court.

### What is the Potential Risk?

This is a new system with a significant backlog of old unpaid fines and infringements. Consequently there is a risk that the outcomes envisaged by the Act may not be achieved in a timely and effective manner.

### What Did We Do?

The operations of the Fines Enforcement Registry of the Ministry were reviewed. In addition the findings of an internal review of the effectiveness of the fines enforcement legislation undertaken by the Ministry were reviewed and utilised for the purposes of the audit.

#### What Did We Find?

The Ministry's internal review found that there had been considerable improvement in the proportion of court fines and police traffic infringements paid on time. For the first 15 months of operation of FER 75 per cent of fines and 95 per cent of infringements were paid on time (compared to 40 per cent and 75 per cent previously). Other findings included:

##### Licence Suspension

There are numerous old outstanding licence suspensions in the system. However, there are no clear policies regarding further follow-up action. The Ministry's internal review found that:

- at June 30, 1996, individual drivers licences under suspension totalled 32 923, of which 15 000 related to fines over 12 months old which had been taken up from the previous enforcement system;
- there were 4 500 suspensions relating to court fines over five years old and traffic infringements over three years old. Of this number, 3 700 were for amounts less than \$500;
- there were 11 000 registered court fines over \$500 with a total value of \$9.5 million which had been outstanding for over six months; and
- the prospect of licence suspension is less effective against offenders who have already received a court imposed suspension or prison term.

##### Warrants of Execution

Under the Act the Registrar may issue a warrant of execution in respect of unpaid court fines. As at April 1997, there were approximately 5 000 matters (currently 8 900) which had been listed for the issue of warrants. However, the warrants had not been issued to the Sheriff. This significant backlog had been caused by an informal policy to limit the number of warrants referred to the Sheriff to a maximum of 20 offenders per day and to only refer warrants for pre-1995 cases where individual offender amounts are greater than \$500. This policy had been adopted due to resourcing and cost effectiveness considerations.

It has also been identified that approximately 60 per cent of warrants are not satisfied due to an inability to obtain current addresses. Some warrants date back to 1987.

##### Debtors Control

The system does not have a debtors control facility and it is not interfaced with the Ministry's financial management and information system. Therefore, the value of outstanding fines and penalties is not easily determined and reported.

### What Does This Mean?

The absence of formal policies for the follow-up of long outstanding licence suspensions and debts and the taking of action to address these issues means that the number of outstanding suspensions and debts will continue to accumulate.

Further, delays in the issue of warrants increases the risk that revenue will not be collected. The longer these issues are not addressed will also result in greater resources being required to undertake future actions.

In addition, the absence of a debtors control does not allow management to regularly monitor the performance of the fines enforcement system.

### What Should Be Done?

The Ministry of Justice should:

- establish policies for the follow-up and resolution of old outstanding licence suspensions;
- establish priorities and criteria for the issue of warrants of execution;
- establish policies for the extinguishment of old outstanding debts where it is not likely that warrants held by the Sheriff can be executed;
- review resourcing of the Sheriff for the execution of warrants; and
- establish a debtors control within the Registry system.

## FINANCIAL CONTROLS AT AUTONOMOUS COLLEGES

### Area of Concern

The enactment of the *Vocational Education and Training Act* on January 1, 1997 created 11 colleges as statutory authorities autonomous of the Western Australian Department of Training (the Department).

These 11 colleges provide vocational training to 122 000 students and manage expenditure of around \$209 million. Separate financial statements and performance indicators reporting on managements' stewardship of these colleges will be prepared for statutory audit for the first time at December 31, 1997.

### What is the Potential Risk?

The Boards of Management of these colleges have implemented financial and operational systems to facilitate independent financial management and reporting. On January 1, 1997 relevant assets and liabilities were transferred from the Department to these colleges. Due to the significance of these changes there is a risk that systems control weaknesses may be undetected and not all assets and liabilities transferred will be brought to account. Both of these risks could lead to delays in preparing reliable annual financial statements at December 31, 1997.

### What Did We Do?

A sample of three colleges was selected to review:

- adequacy of monthly financial and performance reporting;
- key reconciliations, including payroll, debtors and bank;
- asset management; and
- compliance with key Treasurer's Instructions and other controls.

### What Did We Find?

In reading the findings reported below it is important to note that any problems found in one college do not necessarily reflect a problem elsewhere in the system. However, all colleges should review these findings for continuous improvement.

Whilst the review found that the financial controls examined generally complied with relevant statutory requirements, the following areas needed attention:

### Management Reporting

Periodic financial reports are produced for most levels of College management. However, their quality and usefulness varied with reports not including commentary or analysis of the reported figures. Financial reports were not accrual based and there was often no evidence of the reports being regularly used for decision making.

### Payroll

#### *Validity of Payroll*

At one college, business unit managers were not provided with reports to facilitate checking of payroll accuracy whilst at another college, reports were produced but there was no indication they had been checked. Also, regular reports of staff commencements were not produced.

#### *Salary Overpayments*

Significant outstanding balances arising from salary overpayments exist. At one college outstanding balances had increased by 71 per cent to \$52 000 between January and June 1997.

At another college, 70 per cent of debts related to salary overpayments (averaging \$1 047 per employee) and had been outstanding for more than 120 days.

### Asset Management (excluding land and buildings)

#### *Reporting of Assets*

- Reconciliation of asset registers to general ledgers had not been completed during the first seven months of 1997.
- A stocktake had not yet been completed. In some instances, a full stocktake was not performed at December 31, 1996, the date on which the autonomous colleges were established.

#### *Capitalisation of Library Materials*

The purchase of library books is currently expensed by colleges. These materials generally have significant value and a useful life of several years. Accordingly, this accounting treatment warrants review.

### Purchasing and Disbursements

Several instances were identified where written quotes were not obtained for purchases and services over \$5 000. Evidence of proper quotation procedures was generally poor and not in compliance with State Supply Commission policies.

#### What Does This Mean?

These issues, if left unaddressed, increase the risk of error, misstatement and delays in the preparation of accurate annual financial statements. Specifically:

##### Management Reporting

It is not obvious that management outside the finance branch is obtaining optimal benefit from management reports.

##### Payroll

Invalid or incorrect remuneration payments may occur and remain undetected. Where salary overpayments are not managed as a separate class of debtor, there is a risk that follow up will be impeded and such debts will continue to be unacceptably high.

##### Asset Management

The general ledger records of asset holdings may be incorrect and lead to material error in the annual financial statements in relation to non-current assets and related depreciation expense.

##### Purchasing and Disbursements

Colleges may not be able to demonstrate they have received the best value for money.

#### What Should Be Done?

Colleges should review their financial reporting and control systems to assure that they will facilitate the preparation of accurate financial statements. In particular it is recommended that:

##### Management Reporting

- management reports include appropriate explanatory notes, summaries and conclusions on financial and operational performance; and
- colleges move towards routinely producing accrual based financial management information.

##### Payroll

- management be provided with fortnightly payroll listings for their staff and these reports be signed off as evidence of review;
- salary overpayments be reported to management and actively managed; and
- unless exceptional circumstances exist, salary overpayments be recouped over a significantly shorter period perhaps at least at the same rate at which the overpayments occurred.

### Asset Management

- asset registers be reconciled to general ledgers on a monthly basis;
- full stocktakes be completed as a matter of priority; and
- colleges record library materials on a basis similar to that adopted by Western Australian universities.

### Purchasing and Disbursements

- colleges comply with all State Supply Commission policies including obtaining written quotes being obtained for all significant purchases.

## RECENT REPORTS

Details of Reports issued by the Office of the Auditor General prior to the dates below are available from the OAG Reporting and Communications Branch Telephone 9222 7577.

### 1996

#### Tabled

Improving Road Safety – Report No 1	May 1, 1996
First General Report 1996 – Report No 2	May 8, 1996
The Internet and Public Sector Agencies – Report No 3	June 19, 1996
Under Wraps! – Performance Indicators of Western Australian Hospitals – Report No 4	August 28, 1996
Guarding the Gate – Physical Access Security Management within the Western Australian Public Sector – Report No 5	September 24, 1996
For the Public Record – Managing the Public Sector’s Records – Report No 6	October 16, 1996
Learning the Lessons – Financial Management in Government Schools – Report No 7	October 30, 1996
Order in the Court – Management of the Magistrates’ Court – Report No 8	November 12, 1996
Second General Report 1996 – Report No 9	November 20, 1996

### 1997

On Display – Report No 1	April 9, 1997
The Western Australian Public Health Sector – Report No 2	June 11, 1997
Bus Reform – Report No 3	June 25, 1997
First General Report – Report No 4	August 20, 1997
Get Better Soon – Report No 5	August 27, 1997
Waiting for Justice – Report No 6	October 15, 1997

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