2001 (No. 3)

2001

PARLIAMENT OF TASMANIA

AUDITOR-GENERAL SPECIAL REPORT No. 35

SOFTWARE LICENSING

April 2001

Presented to both Houses of Parliament in accordance with the provisions of Section 57 of the Financial Management and Audit Act 1990

By Authority:

Government Printer, Tasmania

Auditor-General's reports are available from the Tasmanian Audit Office, HOBART. This report and the recent titles shown at the back of this report can be accessed via the Office's home page. For further information please contact:

Tasmanian Audit Office
GPO Box 851
Hobart
TASMANIA 7001

Phone: (03) 6233 4030, Fax (03) 6233 2957
Email:- admin@audit.tas.gov.au
Home Page: http://www.audit.tas.gov.au

This report is printed on recycled paper.

ISBN 0-7246-4766-X

10 April 2001

President
Legislative Council
HOBART

Speaker
House of Assembly
HOBART

Dear Mr President
Dear Mr Speaker

PERFORMANCE AUDIT NO. 35
SOFTWARE LICENSING

This report has been prepared consequent to examinations conducted under section 44 of the Financial Management and Audit Act 1990, for submission to Parliament under the provisions of section 57 of the Act.

Performance audits seek to provide Parliament with assessments of the effectiveness and efficiency of public sector programs and activities, thereby identifying 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 Tasmanians.

Yours sincerely

A J McHugh
AUDITOR-GENERAL

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

Aurora	Aurora Energy Pty Ltd
BSAA	Business Software Association Of Australia
DPIWE	Department of Primary Industry, Water and Environment
DJIR	Department of Justice and Industrial Relations
Forestry	Forestry Tasmania
GBE	Government Business Enterprise
GITC	Government Information Technology Conditions
IT	Information technology
MITS	Managed Information Technology Solutions
PC	Personal computer
SOC	State owned company

INTRODUCTION

Under the provisions of section 44(b) of the *Financial Management and Audit Act 1990* the Auditor-General may

> "carry out examinations of the economy, efficiency and effectiveness of Government departments, public bodies or parts of Government departments or public bodies".

The conduct of such audits is often referred to as performance auditing.

This report relates to a performance audit carried out by the Tasmanian Audit Office during the period November 2000 to March 2001.

The objective of this performance audit was to assess the effectiveness and efficiency of public sector management of software licensing in Tasmania.

The approach taken in this audit was to conduct field visits to two government departments, a government business enterprise (GBE) and a state owned company (SOC).

AUDIT OPINION

Report Title	Software licensing
Nature of the Audit	The objective of this performance audit was to assess the effectiveness and efficiency of public sector management of software licensing in Tasmania.
Responsible Party	Department of Primary Industry, Water and Environment Department of Justice and Industrial Relations Forestry Tasmania Aurora Energy Pty Ltd
Mandate	This audit has been carried out under the provisions of section 44(b) of the *Financial Management and Audit Act 1990* which provides that: *'The Auditor-General may carry out examinations of the economy, efficiency and effectiveness of Government departments, public bodies or parts of Government department or public bodies.'*
Applicable Standards	This audit has been performed in accordance with Australian Auditing Standard AUS 806 "Performance Auditing" which states that: *"The objective of a performance audit is to enable the auditor to express an opinion whether, in all material respects, all or part of an entity's activities have been carried out economically, and/or efficiently and/or effectively."*
Limitation on Audit Assurance	Audit procedures were restricted to testing of a limited number of software licences. This provides less evidence than would be available by applying more extensive and comprehensive procedures. The evidence provided by these means is persuasive rather than conclusive in nature.
Audit Criteria	The assessment of management of software licensing was ascertained under these criteria: 1 Management's commitment to legal software use. 2 Security of software 3 Monitoring of licence conditions 4 Acquisition and payment
Opinion and Conclusions	On the basis of field work conducted in the four entities reviewed in this audit it was possible to obtain a "snap shot" of the software licensing function undertaken by a range of public sector organisations in Tasmania, encompassing government departments, a government business enterprise and a state owned company. It appeared that a strongly centralised IT function made it easier to administer software licences. Nevertheless, our audit showed that each of the organisations had demonstrated a firm commitment to legal software use. Dishonest or unethical use of software assets was clearly discouraged through policy

statements.

The security of software was generally satisfactory as all auditees with one exception had software registers while all had adequate physical security of software media.

Weaknesses were evident with respect to monitoring the conditions of software licensing agreements and this area needed to be strengthened.

Also, some entities could consider improvements in the way that payments for and management reporting of software licence fees are handled.

PRINCIPAL AUDIT FINDINGS AND RECOMMENDATIONS

Organisations should implement a procedure for all staff to sign an Employee Compliance Statement indicating their agreement to legal software use. Evidence of acceptance should be centrally retained and readily retrievable.

Page 13

Organisations should consider implementing automated tools to aid management of software licences.

Page 19

Organisations should consider developing procedures on spot checks of software on PCs that would include documentation of processes and results.

Page 20

Organisations should consider annual checks of software on PCs, including documentation of processes and results.

Page 20

AUDIT OBJECTIVES, APPROACH AND COST

Audit Objective

The objective of this performance audit was to assess the effectiveness and efficiency of the management of software licensing by departments and government businesses in Tasmania.

Scope of the Audit

The audit focused on the public sector's role of managing software licensing with particular emphasis on the conditions imposed by licence agreements and the degree of auditee adherence to them.

Through our work we aimed to produce a 'snapshot' of current performance by selecting for review a range of public sector bodies reflecting a variety of commercial orientations. The selected sample comprised the following:

Government departments	Department of Justice and Industrial Relations;
	Department of Primary Industry, Water and Environment;
Government business enterprise (GBE)	Forestry Tasmania; and
State owned company (SOC)	Aurora Energy Pty Ltd

Audit Criteria

The following audit criteria were applied to software licensing:

1 Management's commitment to legal software use
   - Do policies exist in relation to software licensing?
   - Does the auditee have a software code of ethics?
   - Do staff sign an Employee Compliance Statement?

2 Security of software
   - Is there a software register?
   - Are original disks and CDs secured?

3 Monitoring of licence conditions
   - Are automated tools available to aid monitoring of licence conditions?
   - Are unannounced spot checks made?
   - Are annual audits of software conducted?
   - What level of documentation is maintained in relation to monitoring?
   - Do equipment disposal procedures have regard to software licensing implications?
   - Have auditee software licence conditions been affected by organisational changes?

4 Acquisition and payment

- Are sound processes used in acquiring the software?
- Has the auditee adhered to the terms of the software licence?
- Do software licence payments made comply with licence conditions?

Audit Steering Committee

In line with established practice for the conduct of performance audits, a steering committee was convened to reflect stakeholder views. The committee provided input to the audit methodology and reviewed the draft report upon its completion. The Auditor-General chaired the steering committee and its members were drawn from the following areas:

- Department of Education;
- Department of Police and Public Safety;
- Department of Premier and Cabinet;
- Department of Primary Industry, Water and Environment;
- Forestry Tasmania;
- Retirement Benefits Fund Board; and a
- Representative of the performance audit section.

Audit Methodology

The following methods were used during the course of the audit to gather evidence from which conclusions were drawn:

Data was gathered through field visits to each of the organisations audited. Documents relating to policies and procedures in relation to software licensing were obtained and analysed.

Discussions were held with staff from the *e*Services Group in the Department of Premier and Cabinet.

Audit Resources and Timing

Planning for the performance audit commenced in October 2000. Field-testing commenced in December 2000 and was completed in February 2001 with the report being finalised in March 2001.

The total cost of the audit, excluding report production costs but including the cost of Tasmanian Audit Office staff is estimated at $31 464.00.

BACKGROUND

From the mid 1980s there has been explosive growth in use of information technology (IT) for all manner of applications in business and industry. Advances have not been restricted to hardware since computers, computer networks and personal computers (PCs) cannot function without suitable software programs. These products comprise systems software (eg operating systems, communications software and database management systems) and applications software (eg financial management, asset management and word processing). When a consumer pays for software the transaction is not a purchase but an agreement to use a licensed product under the terms of certain licence conditions.

Software licenses exist in a variety of forms. Some are based on the number of machines on which the licensed program can run whereas others are based on the number of users that can access the program. Sometimes a license allows the program to run on different computers as long as the copies are not used simultaneously. Most PC software licenses permit the program to be used on only one machine and copies of the software to be made only for backup purposes.

As with other forms of intellectual property the creator or vendor holds a copyright over the use of their property with protection extended by the Commonwealth's *Copyright Act 1968.* This Act has been amended a number of times to keep abreast of technological developments and it was updated recently by the *Copyright Amendment (Digital Agenda) Act 2000*. Under the *Copyright Act 1968*, it is illegal:

- To copy software or accompanying documentation without the permission of the copyright owner;
- To run a copyrighted software program on two or more computers simultaneously unless the licence agreement specifically allow this (i.e. a multi-user or site licence); and
- To withhold knowledge that the criminal law against unauthorised software copying is being breached.

Breaches of the Act can incur substantial fines, which for organisations could be as high as $300 000 or for individuals up to $60 000 plus imprisonment. As well as criminal convictions there is also the possibility of civil action by software companies seeking damages. In Australia these companies have a voice through the Business Software Association of Australia (BSAA).

The BSAA is part of an international industry association that operates in more than 60 countries to combat illegal copying and use of software. Research undertaken by BSAA in 1989, the year that it was established, found that at least 50 per cent of PC software used in Australia was unlicensed (i.e. illegally copied). Campaigns of education and litigation have reduced this level but a study in 1996 estimated illegal software use was still at 32 per cent, a rate that is higher than other Western countries. Further BSAA estimates put the cost of software theft to industry at more than $290m annually in lost sales.

As part of the strategy to safeguard their industry's interests, BSAA has sought to raise the level of public consciousness on licensing issues. One initiative has been the publication of a guide ('Software Compliance and Audit Manual') that helps organisations to understand and meet their legal obligations and thereby reduce the risk of costly and embarrassing legal action.

With respect to government organisations, management of software licences can be viewed as a matter of ensuring that they have the correct quantity. Too little in the way of licences

can cause situations such as unauthorised use, theft and breach of licence conditions. Conversely, too many licences represent over-expenditure and consequent waste of government resources. Effective management hinges on maintaining the right balance.

Audit Focus and Approach

Against this background, the objective of our audit was to assess the effectiveness and efficiency of public sector management of software licensing in Tasmania. Through our work we aimed to produce a 'snapshot' of current performance that would allow an opinion to be formed as to the extent to which organisations were complying with their legal obligations under software licence agreements and the *Copyright Act 1968*.

The State Service has no specific guidelines that cover management of software licences, thus the auditees have been required to develop their own approaches to this potentially complex issue. The ways in which this obligation has been met reflect the diverse business environments of the auditees as well as the scale and complexity of their organisational structures.

Reviews and Audits in other Jurisdictions

In Victoria, Special Report 23 'Information Technology in the Public Sector' was tabled in 1993. The overall objective of the audit was to ascertain the extent to which illegal and unauthorised software existed on microcomputers within the public sector and to determine whether existing policies and procedures were effective in the detection and prevention of its use. Findings made in this report included the following:

- Licences or proof of ownership could not be produced for 25 per cent of the software loaded onto the microcomputers examined;
- Of the microcomputer software used, 34 per cent had not been authorised by the organisations and a significant proportion of this software, e.g. games, was not related to their business activities; and
- Viruses were detected in 2 of the 6 auditees reviewed.

More recently the Office of the Auditor-General of Western Australia published "Public Sector Performance Report" Report No 1 - April 2000. The following findings were made in this report:

- The extent to which software use was monitored varied between organisations with some incurring higher licence fees than were necessary;
- Difficulties were experienced in locating contract documentation for current software contracts;
- Payments for software were not being checked against contracts and pricing schedules; and
- There was no evidence that standard vendor contract provisions had been vetted by legal officers.

FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

This section of the report deals with our findings, conclusions and recommendations made in relation to the audit criteria.

Organisations Audited

Department of Justice and Industrial Relations (DJIR)

DJIR is responsible for a diverse range of functions encompassing Courts, Tribunals and Statutory Officers as well as administrative support services at the corporate level. Methods employed to monitor and control software licensing are influenced by this diversity as well as the need to recognize the autonomy of the areas within the department that are separately accountable to Parliament.

Information Technology Services (ITS) is a section in the corporate centre providing infrastructure support for the department's IT network (comprising approximately 550 PCs) including maintenance and upgrading of the PC standard operating environment. The section's responsibilities cover standards for supported desktop hardware, software and issues such as anti-virus activities and licensing.

Business applications specific to an area within DJIR (e.g. financial management information systems, case management systems, records management) were generally the responsibility of the local management rather than ITS. This responsibility extended to ensuring compliance with software licensing conditions.

Department of Primary Industry, Water and Environment (DPIWE)

DPIWE was subject to an 'Awareness, Compliance and Education' review of software asset management practices in 1999. This review, carried out by the firm Deloitte Touche Tohmatsu, retained by Microsoft Corporation, sought to gauge the department's management of its commitments under the Enrolment Agreement with Microsoft.

The subsequent report, which was presented in November 1999, concluded there was a low risk of DPIWE not ensuring that all software licences were being appropriately managed. Nevertheless, a number of recommendations were made aiming at improving processes. Since that time, the department has striven to implement the recommendations although some aspects were still in progress at the time of our review. At the time of the audit DPIWE's complement of PCs was approximately 1 450.

GBE: Forestry Tasmania (Forestry)

The Information Technology Branch at Forestry was part of the corporate centre and exerted a strong coordinating role within the enterprise. As the smallest of the organisations reviewed (comprising approximately 400 PCs), effective central control was easier to achieve than may have been possible in a larger entity.

An internal audit of IT controls had been conducted by KPMG in March 2000 that included a review of software licence management. The only finding reported on this subject was that a software register should be established. Management accepted the finding agreeing that it would be implemented by the end of May 2000.

SOC: Aurora Energy Pty Ltd (Aurora)

Prior to disaggregation, the Hydro-Electric Corporation (HEC) had had its own in-house information technology unit (Information Technology Services and Solutions - ITSS). After Aurora was established under the *Electricity Companies Act 1997* it continued to rely on services obtained from ITSS under a commercial arrangement with Hydro Tasmania. Consequently, Aurora inherited these policies, procedures, systems and infrastructure. Meantime Hydro Tasmania disbanded ITSS preferring instead to outsource its IT function.

Subsequently, the Tasmanian Electricity Supply Industries (Aurora, Hydro Tasmania and Transend Networks Pty Ltd) decided to jointly source their IT infrastructure services from a single provider in order to satisfy their common needs by January 2000 (for transition not later than 1 July 2000). A contract was awarded to the firm MITS (a unit of the international enterprise Logica) with effect from 1 July 2000.

So far as interaction with the contactors is concerned, Aurora develops specifications for its IT environment and MITS provides advice and a cost assessment for proposals submitted. After this process of consultation Aurora arranges acquisition of the recommended software with business units funding the expenditure from their own budgets. At the time of the audit Aurora had approximately 650 PCs.

Performance Against Audit Criteria

1 Management's commitment to legal software use

Recognition of obligations under the *Copyright Act 1968* should be addressed by senior management and unequivocally communicated throughout an organisation. To do so is not just a protection against legal action but an opportunity to reinforce the organisation's commitment to ethical standards of business.

Specifically, to test auditees' commitment to legal software use our criteria sought to establish whether:

1. Policies existed in relation to software licensing;
2. The auditee had a software code of ethics; and
3. Staff signed an Employee Compliance Statement.

1.1 Do policies exist in relation to software licensing?

Software licensing policies were evident at each of the entities. In some cases the policies contained background or explanation of their underlying principles. Also, some had a wider focus incorporating issues such as web browsing, e-mail and general computer usage. Endorsement by senior or executive management groups (comprising the Chief Executive Officer and general managers) was a common feature.

Web start up pages were sometimes used to display these policies making them readily accessible to staff. These included sections that dealt with the auditee's interpretation of 'Acceptable Use' that required users to read, understand and agree to the principles espoused. Specific examples of unacceptable uses related to software were:

- Downloading or installing unlicensed software, and
- Intentionally copying any software.

At Aurora, management had completed a review of the policies, processes and controls inherited from the HEC with the objective of identifying deficiencies and developing or amending policies as required.

Each of the auditees was rated as satisfactory.

1.2 Does the auditee have a software code of ethics?

The BSAA recommends a number of initiatives for senior management to deter software theft. Adoption of a software code of ethics is one of these actions and a suggested format that could be used within organisations is included in the 'Software Compliance & Audit Manual' (refer to Appendix 1). Although each of the auditees did have a commitment to the legal and ethical use of software none had a separate charter. However, overlap was found between some of the principles of BSAA's model code of ethics and elements contained in usage policies reviewed. As an example, paragraph 4 of the BSAA model code of ethics states:

> 'We will enforce strong controls within our organisation to prevent the making or use of unauthorised software copies. This will include effective measures to verify compliance with these standards and appropriate disciplinary action for any violation of these standards.'

Aurora's 'Acceptable Use Policy' clearly indicates that inappropriate use of the electronic information service is contrary to the 'Code of Personal Conduct' and will result in disciplinary action. In such cases the seriousness of the breach would determine the level of disciplinary action imposed. Forestry notifies employees that failure to comply with the stipulated conditions may lead to disciplinary action including termination of employment. The two departments did not explicitly mention disciplinary action in relation to breaches of acceptable use guidelines but their ethical principles were implicit in the examples provided to illustrate acceptable or appropriate use of information resources.

Accordingly, we found that even though the auditees did not have documents specifically titled 'Code of Ethics' their principles were unambiguously communicated to employees and that each of them met this audit criterion.

1.3 Do staff sign an Employee Compliance Statement?

Another recommendation aimed at deterring software theft proposed by BSAA in the 'Software Compliance & Audit Manual' is that organisations use 'Employee Compliance Statements'. These provide evidence that employees have been made aware of policy on software use and are also aware of the implications of the law, namely the *Copyright Act 1968.*

Organisations' performance with respect to this audit criterion varied. Examples of statements used by the auditees are shown in Table 1, below.

Table 1: Employee Compliance Statements

Auditee	Source	Obligates Employee to:
Department of Justice and Industrial Relations	Intranet site Web browsing, e-mail and computer use policy: Acceptable use principles	'Respect[ing] intellectual property rights'
Department of Primary Industry, Water and Environment	Departmental Software/Data Acceptable Use Agreement	'Adhere to copyright law regarding use of software, information, and attributions of authorship'
Forestry	Information System Access Request Form	'Not install unlicensed or pirated software (including games)'
Aurora	Acceptable Use Policy	[Refrain from] 'Using copyrighted material without permission'

As the wording of the statements differed so did the extent of implementation between the auditees. One was intending to introduce an agreement as part of the induction process for new employees but had not yet done so. Two others did have types of employee compliance statement but they were incompletely implemented in the organisations. That is, they had been obtained from employees who had commenced work after a particular date but did not apply to staff already employed. The tactic adopted by one of these two entities to cover existing employees was to rely on a reminder message that appeared on screen whenever they logon to a file server. The message stated:

> 'Do not attempt to logon unless you are an authorised user. In using this PC you agree not to download, install or run unlicensed software.'

Although such on-screen messages convey information they do not provide irrefutable evidence of employees' acknowledgement of and agreement to the conditions since there is nothing to indicate that employees have read or understood the contents.

At the heart of this audit criterion there are two linked concepts, firstly that an employee has been made aware of the conditions that apply to access to and usage of an auditee's computer systems and secondly that evidence of their acceptance is available. These goals may be met through paper-based systems or alternatively via electronic means, as for example where passwords can only be changed after acknowledgement of usage conditions and a record of the acknowledgement can be retained on log files.

Recommendation

Organisations should implement a procedure for all staff to sign an Employee Compliance Statement indicating their agreement to legal software use. Evidence of acceptance should be centrally retained and readily retrievable.

Only one auditee had a fully implemented procedure and this was integrated with the assignment of user IDs. In practice, this meant that the IT section would not grant access to the computer network unless an agreement form, authorised by the employee's manager, had been received in the IT section.

Summary – Audit Criterion 1

	Aurora	Forestry	DPIWE	DJIR
Licensing Policies?	✓	✓	✓	✓
Code of Ethics?	✓	✓	✓	✓
Signed Employee Compliance Statement?	Partial use of forms	✓	Forms for new employees and on screen reminders	On screen reminders for employees

Conclusion - Audit Criterion 1

Senior management of the entities reviewed had demonstrated an unconditional commitment to legal software use. This took different forms but it was evident that deliberate actions had been planned and executed. In some cases there was room for improvement and plans had been made to update or extend aspects of policy frameworks in regard to software licensing.

2 Security of software

Businesses routinely attend to security when it relates to assets such as cash, business equipment and intellectual property. Protection of assets calls for physical security combined with the establishment and maintenance of accurate records: this is no less true of software assets. Secure storage and controlled access to the original program source such as CDs together with the recording of acquisitions are important elements in deterring or preventing theft.

In order to confirm the extent to which software security was managed our audit posed the following questions:

1. Is there a software register? and
2. Are original disks and CDs secured?

2.1 Is there a Software Register?

Central control of the IT function was displayed to a greater or lesser extent in the organisations under review. Each had a separate business unit or responsible officer in the corporate area that was given carriage of IT issues. Consequently, decisions as to composition of the standard operating environment, and the organisation's attitude to non-standard software could be made centrally and applied uniformly. This centralised approach was also evident in the acquisition of software with the process either carried out centrally by IT sections or alternatively co-ordinated and approved by them. Having this degree of central control made the use of software registers a straightforward matter and all but one of the auditees had a software register in operation.

Typically, registers held data that included asset identification, acquisition details and user coding for management reporting. In the event that any further particulars that were not currently in the database were required (eg discounts, pricing particulars, etc) the source documents for the data held in the software register were available in the IT area and were readily accessible to provide that information.

DJIR

Compared to the other auditees, there appeared to be less central control of the IT function at DJIR and a software register had not been implemented. The source documents were on hand that would enable one to be produced, although it would be a difficult task in respect of software installed on some older PCs. Over the last two to three years the number of PCs deployed by the department had more than doubled to well over 500 and while record keeping in respect of the newer machines was satisfactory the situation with those acquired earlier was not so clear.

Rather than having a single integrated standard operating environment a variety of types of Microsoft products were in use across the department. DJIR held licences for both Office 95/97 and Office 2000, Exchange 4/ 5 / 5.5 and 2000 CALS and NT 4 although the products actually in use were Office 95, Exchange 4 and Windows NT.

Windows 95 will not be supported beyond June 2001 and the IT section aimed to use this time prior to the enforced generational change as an opportunity to consolidate documentation for the Office 2000 environment with DJIR's software assets.

The department had a detailed hardware register that had records of PCs together with printers and other ancillary equipment. It was constructed with fields to track software but this information had not yet been input. When complete, it would be possible to establish a software register that would aid management of software licensing by sorting and extracting the relevant hardware data.

Recommendation

The Department of Justice and Industrial Relations should develop a software register to manage software licences.

DPIWE

At DPIWE the view was taken that an inventory system should be available to allow software to be managed throughout its life cycle from purchase, installation through upgrade or re-location to final disposal. The 'life cycle' approach was undertaken so that it would enable the department to:

- Effectively use these assets;
- Be confident that it could locate its assets; and
- Operate its software assets in compliance with licence conditions.

The department's IT area maintained a combined hardware and software register. Details of individual PCs were recorded together with some software although standard operating environment products were not shown for each listing. Since they were uniformly applied across the organisation and the number of licences had to tally with the number of PCs the separate recording of these products was not seen as justified. As the Tasmanian State Government has a volume purchase agreement with Microsoft, printed software licences were not supplied to each entity. To cover the situation of licence documentation not being available DPIWE used financial records (i.e. orders, payments) as evidence of software licences.

FORESTRY

Forestry's software register was established in response to an internal audit recommendation made in early 2000. In line with Forestry's philosophy of centralised IT management, the IT manager controlled the register and it appeared to be an effective tool for managing software licensing.

AURORA

Aurora's 'Policy on Personal Computer Software Licensing' stated:

> 'Responsibility for maintaining a register of software licences associated with the standard operating environment rests with the Manager IT and the IT Service Provider (MITS).'

This requirement formed part of the contract, schedule 1 of which obligated MITS to maintain a register for the standard operating environment. A database of hardware and software had been created at the time of the outsourcing of IT management and this also formed the basis for some charging associated with the Aurora - MITS contract.

A software register for non-standard operating environment products had also been created in line with the requirements of Aurora's policy. An exercise had been carried out after the transition from ITSS to MITS to compile a set of contracts and associated records that reflected software systems in use. This included those that had been in place from the HEC times and were still in operation.

Copies of these 'Third Party Software Agreements' were held by the Group Manager IT and the records management system, while a third copy was retained by MITS. The records were in regular use at Aurora, *inter alia* to certify invoices from software suppliers for payment.

2.2 Are original disks and CDs secured?

So far as the storage of original disks and CDs was concerned, each auditee had satisfactory security for original copies of software media that involved safekeeping in secure areas by IT staff.

Authority to install software was usually restricted to IT staff even in those cases where one-off purchases of software had been made to meet the needs of specialised business units (e.g. scientific or statistical packages).

At DJIR IT staff installed new or upgraded programs related to the standard operating environment onto the relevant servers which were located within a secure area. Some of the business applications that were specific to the various areas of DJIR (e.g. Crown Law; Births, Deaths and Marriages) were managed directly by the software suppliers or through their appointed contractors. In these cases responsibility for the physical security of software media rested with the supplier.

DPIWE's IT manager maintained a library of CDs intended for software installation. For software that was outside of the standard operating environment and acquired for a specific business need the CDs were held by the IT manager and only released to clients after evidence of software licences had been verified.

Forestry's IT staff installed new or upgraded software onto the server which was then made available to users via a software management tool. Access to particular software was tied back to the procedure covering employee compliance statements referred to in section 1.3. Once installed on Forestry's network the original CDs became in effect back up copies and could be used to re-install software if needs be.

In the case of Aurora, it passed on software that had been acquired to MITS since that company was required to install and maintain software under the terms of the contract. Subsequently, MITS also provided storage and security for the software supplied by Aurora.

We found that each of the auditees had met this audit criterion.

Summary – Audit Criterion 2

	Aurora	Forestry	DPIWE	DJIR
Software Register?	✓	✓	✓	×
Includes standard operating environment software?	✓	✓	✓	N/A
Includes non-standard operating environment software?	✓	✓	✓	N/A
Original disks and CDs secured	✓	✓	✓	✓

Conclusion - Audit Criterion 2

Only one auditee did not have a register of software assets. The physical security of original program sources such as CDs was satisfactory for the auditees reviewed.

3 Monitoring of licence conditions

Having policies in place and attending to physical security are part of the process of deterring or eliminating theft of software in organisations. However, it is also essential to ensure that strict compliance with licence conditions and organisational policy is achieved so ongoing monitoring is a third element that needs to be instituted.

Accordingly, our audit sought to identify the extent to which monitoring of licence conditions was undertaken through application of the following sub-criteria:

1. Are automated tools available to aid monitoring of licence conditions?
2. Are unannounced spot checks made?
3. Are annual audits of software conducted?
4. What level of documentation is maintained in relation to monitoring?
5. Do equipment disposal procedures have regard to software licensing implications? and
6. Have auditee software licence conditions been affected by organisational changes?

It should be noted that the above criteria (1–3) reflect a range of monitoring options that could be employed by organisations but that it may not be necessary to implement all three methods to achieve an effective monitoring regime. Whichever method/s are adopted it is important that records are maintained to meet the dual requirements of accountability and transparency in management processes.

3.1 Are automated tools available to aid monitoring of licence conditions?

There are software tools that deal with the distribution and tracking of application software. These include asset management tools to provide organisations with a tally of their

hardware and software as well as determining what model PC an employee has, with how much internal memory, and which software applications are loaded on it. Although the auditees did have some automated tools in place their primary function was not monitoring of licence conditions and little use was made of their monitoring capabilities.

DJIR did not have tools to undertake automated monitoring of software licences. The variations that existed in the standard operating environment would complicate the selection of monitoring and metering tools if the department were to decide to implement such a strategy.

DPIWE had the largest computer network of the organisation's reviewed and did not use automated software licence monitoring facilities. This was in part due to the cost of acquiring tools that would be suitable for a large network but also to the perceived operational difficulties that such products could bring with them (such as slowing up networks). Another influential factor was the management philosophy in relation to software assets. The IT manager's view was that the role of his section was to respond to clients' needs and provide them with the equipment they needed to conduct their business. However, management of these assets was a matter for business unit managers. Where a business unit manager was concerned about software licensing the IT section would provide information or expert advice to support managers.

As mentioned in section 2.2, Forestry used network tools to install software and extend access to users. At the time of the audit, though, automated monitoring and metering of software licences was not possible. However, the IT manager intended to acquire a software monitoring program when a suitable version becomes available which was anticipated to be around mid-2001.

Aurora's IT contractor, MITS, did have software that was able to perform some monitoring functions but it was not yet implemented completely.

A view that was commonly expressed among auditees' IT staff was that illegally installed software would become apparent through operating problems that it could create on their networks. In the absence of problems the assumption was made that everything was running smoothly.

We found that two of the auditees had partially met this audit criterion and two had not.

Recommendation

Organisations should consider implementing automated tools to aid management of software licences.

3.2 Are unannounced spot checks made?

Section 3.2.7 of BSAA's 'Software Compliance and Audit Manual' recommends that:

> 'To ensure strict compliance, your organisation needs to conduct periodic unannounced spot checks of all personal computers ...'

Checks were sometimes made by IT management at DPIWE using network monitoring techniques but these are not a regular feature of IT activities. Rather, such checks were initiated by managers who requested that the PCs of particular employees or groups be checked as the need arose.

None of the auditees had a procedure regarding spot checks to confirm compliance with software licence conditions nor was there any indication that checks had been carried out on an *ad hoc* basis. Despite this, there are activities that IT sections perform that could provide elements of spot-checking. For instance, when PCs are de-commissioned by IT staff it is likely that illegally installed software could come to light.

Also, (as mentioned above in section 3.1) the view that day-to-day workings of IT staff in dealing with users' problems could uncover licensing problems was widely held. However, this should not be relied on in isolation since two criticisms can be levelled against this stance. Firstly, it may be possible that breaches could occur that do not cause disruptions to the operation of an organisation's network and thus remain undetected. Secondly, it puts the emphasis on reacting to situations after they have occurred rather than taking the initiative to prevent breaches from happening in the first place.

With regard to both these activities (i.e. checks at de-commissioning and checks that arise through routine day-to-day actions) there needs to be a record of what has been checked and the results obtained. Similarly, if organisations do implement a regime of specific spot checks a log should be maintained to show which parts of the organisation were examined and when, as well as noting the outcomes of the checks.

Recommendation

Organisations should consider developing procedures on spot checks of software on PCs that would include documentation of processes and results.

3.3 Are annual audits of software conducted?

Section 3.2.7 of BSAA's 'Software Compliance and Audit Manual' further recommends that:

> 'At least once per year, a comprehensive software audit should be conducted.'

Annual audits had not been performed in any of the entities reviewed.

In line with the 'life cycle' approach referred to in section 2.1, DPIWE was in the process of introducing a system of that would allow auditing of software licence compliance. The IT manager was in the throes of assigning responsibility for the function to business unit managers. They in turn would be held accountable for any licensing variances detected. Business unit managers will receive a listing of software assets in use by their area every four months that will be based on data contained in the register of hardware and software. Managers will then verify items shown on the inventory reports.

Recommendation

Organisations should consider annual checks of software on PCs, including documentation of processes and results.

3.4 What level of documentation is maintained in relation to monitoring?

This criterion was not applicable because none of the four entities had implemented annual audits or spot-checking procedures.

3.5 Do equipment disposal procedures have regard to software licensing implications?

Disposal of existing hardware has the potential to impact on licensing issues. Where software licences are held in respect of the whole organisation or large part of it the return or disposal of hardware would necessitate unloading software from the machine before selling or re-assigning it with whatever notation is appropriate. On the other hand, if the licence is specifically in respect of the particular PC the licence could be transferred with it.

The majority of DJIR's PCs were leased and there was a steady flow of older machines back to the IT section for decommissioning. This process included the removal of all software at which time unauthorised software could come to light. On receipt of the replacement PC the

standard operating environment would be installed and the number of licences would be balanced through the process of 'ons and offs'.

DPIWE coordinated the acquisition and disposal of hardware using a systematic approach. PCs at particular sites were replaced *en masse* rather than piecemeal, conferring the advantage of uniformity that made the IT section's support role more straight forward. This method also had advantages for planning software upgrades because they could be integrated with the arrival of new generations of PCs. Further, a pre-determined number of old licences can be replaced with new versions in a synchronised fashion.

When Forestry disposed of PCs only the operating system was left in place, thus avoiding software licensing problems. For those software packages that require licence key numbers advice was conveyed to the suppliers. Processing of 'ons' and 'offs' of software on changed over hardware was done via a network management tool.

In the case of Aurora, when PCs were to be replaced MITS de-commissioned returned machines, reformatting disk drives to original specification, and commissioned new or replacement ones according to the desired configuration of standard operating environment or non-standard products required.

We found that each of the auditees had met this audit criterion.

3.6 Have auditee software licence conditions been affected by organisational changes?

In the public sector sections or divisions of an organisation are sometimes split off and set up as separate entities, combined with existing entities or moved between the different tiers of government. Accommodating such changes is a challenge to management and it may also create difficulties with software licensing issues. This kind of major change would need to be treated on a case-by-case basis because of the complexities and peculiarities of each situation. The audit sought to examine whether there had been recent organisational changes and if so how the auditees managed software licensing.

During 2000 the office of the Anti-Discrimination Commissioner had been transferred from the Commonwealth to DJIR. In this instance there was no potentially confusing transfer of software licences because new computers were leased and additional licences acquired in response to the need.

To date, the impact of organisational change had not been a problem for software licensing at DPIWE. The fusion of the former entities that were the forerunners of the department had been accommodated by IT management. The only unit of DPIWE that was not supported was the Royal Tasmanian Botanical Gardens.

Forestry had not been subject to organisational changes on a scale that would have implications for software licensing.

At Aurora the transfer of the regulatory function to the Office of the Tasmanian Electricity Regulator had no impact so far as software licensing was concerned.

We found that each of the auditees had met this audit criterion.

Summary – Audit Criterion 3

	Aurora	Forestry	DPIWE	DJIR
Automated monitoring tools?	Partial	Partial	Partial	×
Unannounced spot checks?	×	×	×	×
Annual software audits?	×	×	×	×
Documentary evidence?	NA	NA	NA	NA
Software removed on disposal?	✓	✓	✓	✓
Licenses affected by organisation changes?	✓	✓	✓	✓

Conclusion - Audit Criterion 3

Monitoring of software licensing conditions needs to be improved at all entities. Consideration should be given to introducing automatic monitoring, spot checks and annual audits to re-enforce management's commitment to legal use that is evident at the policy level. Documentation should be available to indicate what has been done so that issues of transparency and accountability are met.

4 Acquisition and payment

The last of our audit criteria concerned accounts payable processes used for software licence payments. To allow an opinion to be formed the following criteria were used:

1. Are sound processes used in acquiring the software?
2. Has the auditee adhered to the terms of the software licence? and
3. Do software licence payments made comply with licence conditions?

4.1 Are sound processes used in acquiring the software?

To assist government organisations in the acquisition of information technology - whether hardware, software or consultancy services – a standardised process has been developed. The resulting document is known as the Government Information Technology Conditions (GITC). It was produced at the federal level with input from the states and is accepted as best practice for government instrumentalities across Australia.

At DJIR matching of software acquisitions to operational needs was partially supported by the IT section where advice was given to business units on hardware assets that they held. Within the classification of accounts a code was used to separately identify software licensing expenses. Reports were generated for individual budget centres but the IT section did not have the role to supervise acquisitions or centrally coordinate them. It was

understood that the executive management group had a policy on central purchasing of IT equipment but this had not been fully implemented.

Extensive use of GITC contracts was evident at DJIR and official orders from the department, whether for hardware or software, made reference to relevant clauses in GITC.

DPIWE made software acquisitions under the Department of Treasury and Finance's IT common use contract (C150) that conformed to the standardised process developed under GITC.

Where a need existed for specific business software (e.g. mapping) the business unit approached the IT section where the purchase of the desired product was arranged. Appropriate budget centre codes were used to ensure that the expenditure was charged to the user's area. Using this arrangement IT management was able to maintain centralised control while being responsive to the needs of its clients.

Where a GITC contract was available it was "piggybacked" by Forestry to provide the commensurate benefits and evidence was sighted of suppliers adhering to GITC processes. In other cases where GITC contracts were not used in-house legal advice was sought before signing agreements with software suppliers.

As mentioned above in section 3.4, the IT manager advises budget centres of their cost profile for software licences in the coming financial year, thus providing a degree of matching of software acquisitions to operational needs.

Where a need existed for non-standard operating environment software products (e.g. desktop publishing) at Aurora the relevant business unit had authority under the 'Policy on Personal Computer Software Licensing' to select appropriate software. Would-be purchasers were then required to approach MITS for advice as to the compatibility of the desired product with Aurora's network. Independent legal advice on contract terms and conditions was sought. Appropriate coding was used to ensure that the expenditure was charged to the user's budget.

We found that each of the auditees had met this audit criterion.

4.2 Has the auditee adhered to the terms of the software licence?

For applications used in DJIR's business units adherence to the terms of software licences was monitored and appeared satisfactory.

In the case of the IT section, efforts had been made to adhere to software licence conditions in respect of the standard operating environment as well as other products (e.g. Oracle) under its control. The lack of a software register, however, made it difficult to gauge the state of licensing. In order to avoid non-compliance a conservative approach had been taken so that it was more likely that the department held more licences than required rather than too few. As an example, the software licences acquired for the now completed Gilewicz enquiry had been retained.

Recommendation

DJIR's IT records should be improved to ensure that monitoring of software licensing can be more effectively managed.

At DPIWE, agreements with software suppliers were kept on hand in the IT section and regularly accessed. The coordinated, centralised control of IT appeared to have been effective in maintaining adherence to software licence conditions. This had been further strengthened by actively involving business units in managing their own software assets.

Agreements between software vendors and Forestry were retained and oversighted by the IT branch centrally and there appeared to be adequate control of adherence to licence conditions.

Aurora's third party agreements with software suppliers were kept by the Group Manager IT and staff of the Management Accounting section who accessed them during the account authorisation process. Licence fees for products within the standard operating environment are the responsibility of MITS and are included in the contractual payments made by Aurora. Assigning this task to MITS was consistent with the provisions of the contract that required the firm to also maintain the software register for these products. As a result of these arrangements there appeared to be adequate control of adherence to licence conditions.

We found that this audit criterion was met by a majority of auditees.

4.3 Do software licence payments made comply with licence conditions?

At each of the auditees reports were obtained from the financial management information system for software licence expenditure in the current year. A sample of transactions was then selected based on those with the highest monetary values. These were examined to see whether the accounts were paid against the current contract, what process of authorisation was used and whether the expenditure was accurately coded.

At DJIR there was no central control of payment of software licence fees. The IT branch processed and authorised invoices in respect of the standard operating environment and associated network applications. Business managers were responsible for software that was specific to their line of business. In either case, invoices were verified against vendors' licence conditions prior to authorisation for payment. No errors were noted in the selected sample nor with the expenditure coding.

DPIWE's method of account authorisation was similar to DJIR's in that there was a split between responsibility for standard operating environment and other software. Payment was made by the responsible business unit for software used by it, while the IT section paid for the standard operating environment and related products. Verification against contract documentation held on file was evident in both situations.

One of the examples examined involved a digital photogrammetric workstation with a value of $76 351. The items comprising this amount were incorrectly apportioned between accounts for computer hardware and software costs. Although this was not a major problem it did misrepresent the purchase. For equipment where the software and hardware components were integrally linked and in practical terms cannot be physically separated (as is the case with some printers) it may have been more useful to code the entire acquisition as a hardware item.

Forestry's software licence fees were centrally paid in the IT branch with invoices verified against vendors' licence conditions prior to payment approval. However, one payment was noted where central authorisation had been bypassed and an account was paid directly by a business unit without reference to the IT branch. On further examination, the particular software package was not recorded in the software database. The transaction had been coded against the appropriate cost code ('P11 – Software Licence fees') and could have been detected by a process of checking expenditure reports.

Recommendation

Forestry's expenditure reports on cost code P11 (Software licence fees) should be provided to IT branch to ensure that effective central control is maintained.

Aurora's third party software licence fees were paid centrally by the Group Manager IT. Copies of the agreements with software suppliers were filed in Finance & Business and regularly accessed during the certification and authorisation of invoices for payment. Within the financial management information system payments could be identified down to the level of individual contracts. As a further control, the contracts' maximum values were keyed into the accounts payable system to prevent budget overruns when invoices were processed for payment.

Costs input to the accounting system were initially charged to a code in the IT area and subsequently transfer priced to user divisions with the basis for cost apportionment subject to ongoing review. Specific business systems (e.g. Finance, Frontline) were reviewed and checked by the relevant business area, with advice as appropriate from Aurora IT or MITS. However, software licence fees formed part of a bundle of 'corporate charges' advised to users so that licence fees were not separately identifiable, restricting managers' ability to recognise or control them. Depending on the style of management adopted the lack of lower level control of this information may or may not be a problem.

Recommendation

Aurora should consider whether providing users with more detailed reports on software licence fees would allow greater flexibility in controlling resources.

We found that all auditees had met this audit criterion (although a number of recommendations for improvements to the payment process have been made).

Summary – Audit Criterion 4

	Aurora	Forestry	DPIWE	DJIR
Sound acquisition processes?	✓	✓	✓	✓
Adherence to license terms?	✓	✓	✓	✓
Appropriate license payments?	✓	✓	✓	✓

Conclusion - Audit Criterion 4

No problems were noted with software acquisition processes and there were no breaches of the terms of their software agreements in the organisations reviewed. However, some improvements could be made, for example in Forestry's use of financial reports as a trigger to update the software register, at Aurora in providing managers with detailed reports on software costs and in DJIR where creation of a software register would allow more effective control.

OVERALL CONCLUSION

On the basis of field work conducted in the four entities reviewed in this audit it was possible to obtain a “snap shot” of the software licensing function undertaken by a range of public sector organisations in Tasmania, encompassing government departments, a government business enterprise and a state owned company.

It appeared that a strongly centralised IT function made it easier to administer software licences. Nevertheless, our audit showed that each of the organisations had demonstrated a firm commitment to legal software use. Dishonest or unethical use of software assets was clearly discouraged through policy statements.

The security of software was generally satisfactory as all auditees with one exception had software registers while all had adequate physical security of software media.

Weaknesses were evident with respect to monitoring the conditions of software licensing agreements and this area needed to be strengthened.

Also, some entities could consider improvements in the way that payments for and management reporting of software licence fees are handled.

APPENDIX 1

SOFTWARE

CODE OF ETHICS

The unauthorised duplication of copyrighted computer software violates the law and is contrary to our organisation's standards of conduct and business practice. We disapprove of such copying and recognise the following principles as the basis for preventing its occurrence within our organisation:

1. We will neither permit nor tolerate the making or use of unauthorised software copies within our organisation under any circumstances.
2. We will provide in a timely fashion sufficient quantities of legitimately-acquired software to meet all our software needs for all computer hardware.
3. We will comply with all licensing terms and conditions regulating the use of any software we acquire.
4. We will enforce strong controls within our organisation to prevent the making or use of unauthorised software copies. These will include effective measures to verify compliance with these standards and appropriate disciplinary action for any violation of these standards.
5. We will take steps to inform current and future employees of their legal responsibilities in relation to software theft.

.....	.....
Name	*Signature*
.....	.....
Title	*Title*
.....	.....
Organisation	*Date*

Source: Business Software Association of Australia – 'Software Compliance & Audit Manual'

BIBLIOGRAPHY

Auditor-General of Victoria. 1993. *Special Report 23: Information Technology in the Public Sector.*

Auditor-General of Western Australia. 2000. *Report No.1: Public Sector Performance Report 2000*

Business Software Association Of Australia. 2000. *Software Compliance and Audit Manual*

Copyright Act 1968 Commonwealth

Department of Premier and Cabinet. 'The Security of Government Information Resources'. May 2000

Webopedia. 2000. 'Software license', 'Runtime version'. http://www.webopedia.com (29 November 2000)

RECENT REPORTS

1998	**SPECIAL REPORT NO. 25**	**THE YEAR 2000 - ARE WE READY?**
1998	**SPECIAL REPORT NO. 26**	**CAPITALISATION AND REPORTING OF ROAD ASSETS IN TASMANIA**
1998	**SPECIAL REPORT NO. 27**	**USE OF MOTOR VEHICLES IN GOVERNMENT AGENCIES**
1998	**SPECIAL REPORT NO. 28**	**PAYMENT OF ACCOUNTS IN GOVERNMENT AGENCIES**
1999	**SPECIAL REPORT NO. 29**	**COMPETITIVE TENDERING AND CONTRACTING BY GOVERNMENT DEPARTMENTS**
1999	**SPECIAL REPORT NO. 30**	**THE YEAR 2000: COMING READY OR NOT**
2000	**SPECIAL REPORT NO. 31**	**LITERACY AND NUMERACY IN TASMANIAN GOVERNMENT SCHOOLS**
2000	**SPECIAL REPORT NO. 32**	**ASSISTANCE TO INDUSTRY**
2000	**SPECIAL REPORT NO. 33**	**FOOD SAFETY**
2000	**SPECIAL REPORT NO. 34**	**PROCUREMENT IN TASMANIA GOVERNMENT DEPARTMENTS**