Agency Management of Software Licensing

Canberra ACT
17 December 2001

Dear Madam President
Dear Mr Speaker

The Australian National Audit Office has undertaken an across
agency Assurance and Control Assessment audit in accordance
with the authority contained in the *Auditor-General Act 1997.* I
present this report of this audit to the Parliament. The report is
titled *Agency Management of Software Licensing.*

Following its tabling in Parliament, the report will be placed on
the Australian National Audit Office's Homepage—
http://www.anao.gov.au.

Yours sincerely

P. J. Barrett
Auditor-General

The Honourable the President of the Senate
The Honourable the Speaker of the House of Representatives
Parliament House
Canberra ACT

Audit Team

Susan Murray

Contents

Summary and Recommendations

Summary

Background

1.　As at 30 June 2001, the Commonwealth's computer software assets were valued at more than $2.7 billion. Computer software is generally provided under licence. In effect, users are purchasing an agreement to use a licensed product under the terms and conditions of a software licence. The *Copyright Act 1968* provides legal protection for the intellectual property rights of software developers and licensed distributors of software. Under the Copyright Act, it is generally an infringement to copy software without the permission of the copyright owner. Although the Commonwealth cannot be prosecuted for a criminal offence under the Copyright Act, there remains a risk of civil action under the Act for breach of copyright. In addition, there is a need for Commonwealth agencies to comply with any contractual conditions imposed by license agreements.

2.　As in other areas of public administration, Commonwealth agencies are expected to be exemplars of good practice in adhering to the requirements of the law including under copyright and contract. Such a course also avoids the risks to the efficiency and integrity of agencies' computer systems that arise through the use of illegal software. There is also a value for money dimension to this issue because, whilst too few licences can involve a breach of licence conditions, too many licences represents over-expenditure. Accordingly, as with other valuable assets, computer software needs to be managed to mitigate risk and control costs.

Audit approach

3.　The ANAO undertook an Assurance and Control Assessment (ACA) audit[1] of the management of software licensing by five Commonwealth agencies, namely: AGSO—Geoscience Australia; the Australian National University; the Australian Securities and Investments Commission; the Joint House Department; and the Office of Parliamentary

---

[1]　ACA audits are undertaken under the general performance audit provisions of the *Auditor-General Act 1997*. They examine common business activities and processes that are not specifically covered by financial statement or other performance audits. The report to Parliament is generally aimed at improving administration across the Commonwealth public sector. The findings of these audits are indicative, rather than representative, given the relatively small number of agencies involved.

Counsel. The objective of the audit was to provide assurance to these agencies and the Parliament that:

- effective controls are in place to ensure the physical security of software media;
- the risks associated with the use of illegal software are being effectively managed; and
- compliance with software licence conditions is being adequately monitored.

Audit conclusions

4. In terms of the audit objectives, the ANAO concluded that:

- appropriate physical security arrangements were generally in place;
- most audited agencies had implemented a sound control framework to ensure that only licensed software is used within the agency; and
- more comprehensive and regular compliance monitoring activity should be undertaken if agencies are to be adequately assured that preventative controls are effective.

Sound and better practice identified

5. The audit process involved addressing the audit objectives and assessing software management practices against the audit evaluation criteria. It also sought to identify instances of sound and better business practices in the audited agencies. The following sound and better practices were identified:

- maintenance of a software asset register to record details of software items in use and associated licensing information; and
- the secure storage of software in a central area of the agency.

Opportunities for improvement

6. In the light of the audit conclusions and the detailed audit findings communicated to individual agencies,[2] the ANAO has made two recommendations that are of general application to agencies. These recommendations relate to the implementation of software registers and improved compliance monitoring strategies. All audited agencies agreed with both recommendations.

---

2   In addition to this report to the Parliament, ANAO provided a report on the results of the audit to each agency reviewed that included a number of recommendations relevant to that agency.

Software registers

7. The compilation and maintenance of a computer software register assists agencies to ensure that they have the appropriate number of licences for each item of software in use, and are not paying for more licences than they actually need. An effective register will include details of all software items in use, and associated licensing information. Of the audited agencies, two agencies had complete and effective registers in place. A further two had established software catalogues but these catalogues lacked essential licensing information and details of the locations in which software items had been installed. Practices in the fifth agency were variable; some areas had established registers, while others were in the process of developing a register. One impact of this was that those areas that had only recently developed, or just begun developing, a software register, had experienced difficulties in locating licensing records for certain software and there was an increased risk of non-approved software being in use.

Compliance monitoring strategies

8. Ongoing monitoring of compliance with software licensing arrangements is necessary if agencies are to assure themselves that preventative controls are effective. Two key compliance strategies for effective management of software licensing are periodic compliance audits and regular, unannounced spot-checks of software installed on personal computers. These activities assist agencies to: discover illegal and unauthorised software;[3] maintain an accurate and complete accurate record (or register) of hardware and software; and manage software licence costs by minimising unused or surplus licences. Of the five agencies audited, three had undertaken a software compliance audit within the last 12 months with instances of unlicensed software or insufficient licences detected in each case, representing a breach of software license conditions. None of the audited agencies had undertaken a program of spot checking of the software installed on personal computers.

---

[3] Illegal software is software that is unlicensed. Unauthorised software is software that the agency has not approved for use on the agency's computer systems.

Recommendations

Recommendation No. 1
Para 2.9

The ANAO *recommends* that agencies enhance their management of software licensing risks and cost by establishing and maintaining a software asset register to record details of software items in use, and associated licensing information.

Recommendation No. 2
Para 2.17

The ANAO *recommends* that agencies undertake periodic software compliance audits and conduct periodic unannounced spot-checks of software installed on personal computers in order to be assured that preventative controls are effective.

Audit Findings
and Conclusions

1. Introduction

This chapter outlines the importance of sound management of software licensing and outlines the audit approach including its objectives and the criteria applied.

Background

1.1 As at 30 June 2001, the Commonwealth's computer software assets were valued at more than $2.7 billion.[4] Computer software[5] is generally provided under licence. In effect, users are purchasing an agreement to use a licensed product under the terms and conditions of a software licence.[6] The *Copyright Act 1968* provides legal protection for the intellectual property rights of software developers and licensed distributors of software. Under the Copyright Act, it is generally an infringement to copy software without the permission of the copyright owner. Although the Commonwealth cannot be prosecuted for a criminal offence under the Copyright Act,[7] there remains a risk of civil action under the Act for breach of copyright. In addition, there is a need for Commonwealth agencies to comply with any contractual conditions imposed by license agreements.

1.2 As in other areas of public administration, Commonwealth agencies are expected to be exemplars of good practice in adhering to the requirements of the law including under copyright and contract. Such a course also avoids the risks to the efficiency and integrity of agencies' computer systems that arise through the use of illegal software.[8] There is also a value for money dimension to this issue because, whilst too few licences can involve a breach of licence conditions, too many licences represents over-expenditure. Accordingly, as with other valuable assets, computer software needs to be managed to mitigate risk and control costs.

---

[4] Reported as a component of the intangibles asset category in the Consolidated Financial Statements for the year ended 30 June 2001.

[5] The programs, routines and symbolic language that control the functioning and direct the operation of computers are called software.

[6] Software licences 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.

[7] Section 7 of the Copyright Act states that the Act binds the Commonwealth but that nothing in the Act renders the Commonwealth liable to be prosecuted for an offence.

[8] For example illegal software will not be automatically upgraded, there may be difficulties in correcting *'bugs'*, in the absence of user manuals full productivity may not be obtained and it may be incompatible with existing software and/or hardware.

Audit approach

1.3   The ANAO undertook an Assurance and Control Assessment (ACA) audit of the management of software licensing by five Commonwealth agencies, namely: AGSO—Geoscience Australia; the Australian National University; the Australian Securities and Investments Commission; the Joint House Department; and the Office of Parliamentary Counsel. The objective of the audit was to provide assurance to these agencies and the Parliament that:

- the risks associated with the use of illegal software are being effectively managed;
- effective controls are in place to ensure the physical security of software media; and
- compliance with software licence conditions is being adequately monitored.

1.4   Criteria for each audit objective were established to enable an audit opinion to be formed. The relevant legislation, recent work of State Auditors-General[9] and other sources of guidance (including that from the Business Software Association of Australia and the Business Software Alliance[10]) formed the basis for developing these criteria, which are outlined in tables throughout the report.

1.5   In order to form an opinion on agencies' management of software licensing, the audit involved the: identification of controls in place to mitigate the risks associated with the management of software licensing; identification of control and performance gaps; identification of instances of good practice; and recommendations for improvement.[11] Information for the audit was gathered through review of policies and procedures in relation to software licensing, discussions with relevant agency officers and inspection of relevant records.

1.6   The audit was conducted in accordance with the ANAO Auditing Standards. Fieldwork was undertaken between June 2001 and September 2001. The total cost of the audit to the ANAO was $105 000.

---

9   Namely: Office of the Auditor-General of Tasmania, April 2001, *Special Report No.35: Software Licensing*; and Office of the Auditor-General of Western Australia, April 2000, *Report No.1: Public Sector Performance Report*.

10   The Business Software Association of Australia is part of the Business Software Alliance, which is an international industry association of software companies operating in more than 60 countries worldwide to combat illegal copying and use of software.

11   In addition to this report to the Parliament, ANAO provided a report on the results of the audit to each agency reviewed that included a number of recommendations relevant to that agency.

2. Audit Findings

This chapter discusses the findings and recommendations of the audit against the audit criteria relevant to each audit objective.

Agencies' control framework

2.1   Control is a process effected by the governing body of an organisation, senior management and other employees, designed to provide reasonable assurance that risks are managed to ensure the achievement of the organisation's objectives[12]. Most audited agencies demonstrated a firm commitment to ensuring that only licensed software was used within the agency. This commitment was evident through the implementation of a sound control framework. Audit findings in relation to agency control frameworks are summarised in Table 1.

Table 1

Control framework audit findings

Principle	Risks associated with the use of illegal software are being effectively managed.
Audit evaluation criteria	A policy addressing software compliance should be developed and approved.
	Awareness of software management issues should be fostered within an agency.
	Agencies should have effective control over software purchasing activities.
	An agency must have adequate software licences for all items of software in use.
	Software licensing documentation must be retained by the agency.
	Procedures for the installation of software should aim to ensure only legal and licensed software is installed on computer facilities.
	A software asset register should be established and used to record details of software items in use, and associated licensing information.

continued next page

---

[12]   Based on COSO Internal Control—Integrated Framework as amended by NSW Treasury, *Statement of Best Practice, Internal Control and Internal Audit*, June 1995.

Audit findings	Most agencies had implemented a sound control framework including:
	• documented software compliance policies;
	• requiring new users to sign agreements which detail the conditions of use of the agency's IT environment before new users were granted access to the agencies computer network;
	• effective controls over the planning and conduct of purchasing activities, including licensing issues; and
	• IT security restrictions to prevent unauthorised installation of software.
Sound and better practice	The audit noted that some agencies had enhanced their management of software licensing risks and cost by establishing a software asset register to record details of software items in use and associated licensing information.

2.2   Although most agencies were found to have implemented a sound control framework, opportunities for improvement were also identified. For example, most agencies would benefit from a comprehensive software register (see paragraphs 2.4 to 2.8 below). In addition, the ANAO recommended that one agency, whose operating environment and devolved IT administrative arrangements provided different management challenges to the others audited, should make all users aware of, and acknowledge, the conditions that apply to the use of the agency's computer systems in order to reduce to an acceptable level the risk of illegal and/or unlicensed software use.

2.3   **Conclusion:** Most audited agencies demonstrated a firm commitment to ensuring that only licensed software was used within the agency. This commitment was evident through the implementation of a sound control framework including: documented software compliance policies; requiring new users to sign agreements which detail the conditions of use of the agency's IT environment; effective controls over the planning and conduct of purchasing activities, including licensing issues; and appropriate IT security restrictions to prevent unauthorised installation of software.

Software registers

2.4   The compilation and maintenance of a record (or register) of software is an important element in any effective control framework for software licensing. An effective register will include details of all software items in use, and associated licensing information. Without a register, agencies may find it difficult to ensure that they have the appropriate number of licences for each item of software in use, and/or that they are not paying for more licences than they actually need.

2.5   The ANAO found that only two of the five audited agencies had established a complete and effective software register. One agency had long-standing procedures in place to record the details of all new software purchases in the register. The second agency had recently purchased and implemented a software inventory and metering tool. The inventory component of the tool provides an automated listing of the software installed on each personal computer, as well as holding licensing information. When new software items are installed by IT staff, the tool automatically updates its software inventory, with licensing information being entered manually by IT staff. These features mean that the tool is able to provide a complete and accurate software register for the agency.

2.6   A further two of the audited agencies had established software catalogues, which listed the titles of software purchased by the agencies. These catalogues, however, lacked essential licensing information including details of the locations in which software items had been installed.

2.7   Practices in the fifth agency varied. Some areas had established registers, while others were in the process of developing a register. One impact of this was that those areas that had only recently developed, or just begun developing, a software register, had experienced difficulties in locating licensing records for certain software.

2.8   **Conclusion:** The compilation and maintenance of a computer software register assists agencies to ensure that they have the appropriate number of licences for each item of software in use, and are not paying for more licences than they actually need. However, most of the audited agencies had yet to establish a complete and accurate software register.

Recommendation No.1

2.9   The ANAO *recommends* that agencies enhance their management of software licensing risks and cost by establishing and maintaining a software asset register to record details of software items in use, and associated licensing information.

Physical security arrangements

2.10   Secure storage and controlled access to software assists agencies to prevent the theft or misuse of software. Table 2 summarises the audit review of physical security arrangements.

Table 2

Physical security audit findings

Principle	Effective controls are in place to ensure the physical security of software media.
Audit evaluation criteria	Software media should be securely stored.
Audit findings	Appropriate physical security arrangements were generally in place in the audited agencies, although two agencies needed to make some improvements to ensure a consistently high standard of security.
Sound and better practice	Effective controls noted included the centralised storage of software within the IT area, the storage of software within secure cupboards or storerooms and recording the existence and location of software items within the agency's software register.

2.11   Conclusion: Appropriate physical security arrangements were generally in place in the audited agencies.

Compliance monitoring strategies

2.12   Licensing conditions often place limits on the number of users that may concurrently use the software, or on the number of locations in which the software can be installed. If an agency is not monitoring the usage of its software, such licence conditions may be being breached without the agency's knowledge. In addition, without knowledge of actual usage, agencies may be paying more for licences than necessary. In this context, ongoing compliance monitoring is necessary if agencies are to assure themselves that preventative controls (such as user agreements, software registers, sound physical security and restrictions on installation of software) are effective.

2.13   Software compliance audits are generally seen as a key component of an effective compliance strategy. Software compliance audits are a verification process that seeks to identify the software that has been installed and validates that sufficient licences have been acquired for the software in use. Such audits enable agencies to:

- discover illegal and unauthorised software;

- maintain an accurate record (or register) of hardware and software; and

- better manage software licence costs by minimising unused or surplus licences.

2.14 As an adjunct to a program of compliance audits, periodic unannounced spot-checks of software installed on personal computers should be undertaken to identify any unauthorised or illegal software that has been installed. Such checks also provide assurance about the completeness of the software register as well as the effectiveness of IT security restrictions intended to prevent unauthorised staff from installing software.

2.15 Table 3 summarises the audit findings on the subject of compliance monitoring by agencies.

Table 3:

Compliance monitoring audit findings

Principle	Compliance with software licence conditions is being monitored.
Audit evaluation criteria	Software compliance audits should be periodically undertaken. Spot-checks of software installed on PCs should be periodically undertaken.
Audit findings	More comprehensive and regular compliance monitoring activity is needed. In relation to the five agencies examined: • three had undertaken a software compliance audit within the last 12 months with instances of unlicensed software or insufficient licences detected in each case, representing a breach of software license conditions; and • none of the audited agencies had undertaken a program of spot checking of the software installed on personal computers.

2.16 Conclusion: More comprehensive and regular compliance monitoring activity should be undertaken if agencies are to be adequately assured that preventative controls (such as user agreements, software registers and sound physical security) are effective.

Recommendation No.2

2.17 The ANAO *recommends* that agencies undertake periodic software compliance audits and conduct periodic unannounced spot-checks of software installed on personal computers in order to be assured that preventative controls are effective.

Series Titles

Titles published during the financial year 2001–02

Audit Report No.26 Performance Audit
Management of Fraud and Incorrect Payment in Centrelink

Audit Report No.25 Assurance and Control Assessment Audit
Accounts Receivable

Audit Report No.24 Performance Audit
Status Reporting of Major Defence Acquisition Projects
Department of Defence

Audit Report No.23 Performance Audit
Broadcasting Planning and Licensing
The Australian Broadcasting Authority

Audit Report No.22 Protective Security Audit
Personnel Security—Management of Security Clearances

Audit Report No.21 Performance Audit
Developing Policy Advice
Department of Education, Training and Youth Affairs, Department of Employment, Workplace Relations and Small Business, Department of Family and Community Services

Audit Report No.20 Performance Audit
Fraud Control Arrangements in the Department of Agriculture, Fisheries and Forestry—Australia (AFFA)
Department of Agriculture, Fisheries and Forestry—Australia

Audit Report No.19 Assurance and Control Assessment Audit
Payroll Management

Audit Report No.18 Performance Audit
Performance Information in Portfolio Budget Statements

Audit Report No.17 Performance Audit
Administration of Petroleum Excise Collections
Australian Taxation Office

Audit Report No.16 Performance Audit
Defence Reform Program Management and Outcomes
Department of Defence

Audit Report No.15 Performance Audit
Agencies' Oversight of Works Australia Client Advances

Audit Report No.14 Performance Audit
Client Service Initiatives Follow-up Audit
Australian Trade Commission (Austrade)

Audit Report No.13 Performance Audit
Internet Security within Commonwealth Government Agencies

Audit Report No.12 Financial Control and Administration Audit
Selection, Implementation and Management of Financial Management Information Systems in Commonwealth Agencies

Audit Report No.11 Performance Audit
Administration of the Federation Fund Programme

Audit Report No.10 Assurance and Control Assessment Audit
Management of Bank Accounts by Agencies

Audit Report No.9 Performance Audit
Learning for Skills and Knowledge—Customer Service Officers
Centrelink

Audit Report No.8 Assurance and Control Assessment Audit
Disposal of Infrastructure, Plant and Equipment

Audit Report No.7 Audit Activity Report
Audit Activity Report: January to June 2001
Summary of Outcomes

Audit Report No.6 Performance Audit
Commonwealth Fisheries Management: Follow-up Audit
Australian Fisheries Management Authority

Audit Report No.5 Performance Audit
Parliamentarians' Entitlements: 1999–2000

Audit Report No.4 Performance Audit
Commonwealth Estate Property Sales
Department of Finance and Administration

Audit Report No.3 Performance Audit
The Australian Taxation Office's Administration of Taxation Rulings
Australian Taxation Office

Audit Report No.2 Performance Audit
Examination of Allegations Relating to Sales Tax Fraud
Australian Taxation Office

Audit Report No.1 Financial Statement Audit
Control Structures as part of the Audits of the Financial Statements of Major Commonwealth Entities for the Year Ended 30 June 2001

Better Practice Guides

Some Better Practice Principles for Developing Policy Advice Nov 2001

Rehabilitation: Managing Return to Work Jun 2001

Internet Delivery Decisions Apr 2001

Planning for the Workforce of the Future Mar 2001

Contract Management Feb 2001

AMODEL Illustrative Financial Statements 2001 May 2001

Business Continuity Management Jan 2000

Building a Better Financial Management Framework Nov 1999

Building Better Financial Management Support Nov 1999

Managing APS Staff Reductions
(in Audit Report No.47 1998–99) Jun 1999

Commonwealth Agency Energy Management Jun 1999

Corporate Governance in Commonwealth Authorities and Jun 1999
Companies–Principles and Better Practices

Managing Parliamentary Workflow Jun 1999

Cash Management Mar 1999

Management of Occupational Stress in
Commonwealth Agencies Dec 1998

Security and Control for SAP R/3 Oct 1998

Selecting Suppliers: Managing the Risk Oct 1998

New Directions in Internal Audit Jul 1998

Life-cycle Costing May 1998
(in Audit Report No.43 1997–98)

Controlling Performance and Outcomes Dec 1997

Management of Accounts Receivable Dec 1997

Protective Security Principles Dec 1997
(in Audit Report No.21 1997–98)

Public Sector Travel Dec 1997

Audit Committees Jul 1997

Core Public Sector Corporate Governance
(includes Applying Principles and Practice of Corporate
Governance in Budget Funded Agencies) Jun 1997

Administration of Grants May 1997

Management of Corporate Sponsorship   Apr 1997

Telephone Call Centres   Dec 1996

Telephone Call Centres Handbook   Dec 1996

Paying Accounts   Nov 1996

Performance Information Principles   Nov 1996

Asset Management   Jun 1996

Asset Management Handbook   Jun 1996

Managing APS Staff Reductions   Jun 1996