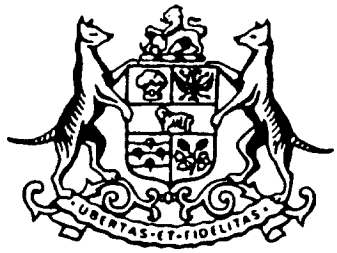

1997

PARLIAMENT OF TASMANIA

AUDITOR-GENERAL SPECIAL REPORT NO 20

Review of Computer Controls in Government Departments

No. 4 of 1997 - June 1997

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

By Authority:

G Priestley, 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 4656 6

TASMANIAN AUDIT OFFICE

19 June 1997

President
Legislative Council
HOBART

Speaker
House of Assembly
HOBART

Dear Mr President
Dear Mr Speaker

PERFORMANCE AUDIT NO 20 – REVIEW OF COMPUTER CONTROLS IN GOVERNMENT DEPARTMENTS

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

Page

SUMMARY OF RECOMMENDATIONS

Protection From Natural Hazards

That agencies take action to minimise the risks to computer equipment from natural hazards.

Security Over Access To The Installation

That agencies develop a security policy, and distribute copies to all staff annually.

That agencies implement the listed computer controls, and in particular the more important controls:

- Restriction on the number of incorrect password guesses allowed,
- Enforced regular change of password, and
- Regular review of access rights.

Network Security

Agencies should periodically review the cost and practicality of implementing encryption on networks.

Backup Of Information

There should be a process of testing tapes to ensure that the backup process is effective and that tapes can be read.

Disaster Recovery Plan

That all agencies give priority to development of a disaster recovery plan.

Recovery From System Failure

That agencies implement incident diaries.

That agencies write recovery procedures for all major systems.

Data Editors

That as far as possible data should only be edited through application menu options.

That where it is necessary to use direct editing of data, appropriate approval and documentation standards be applied.

Change Control

That agencies implement formal processes over change control for important applications.

Segregation Of Duties

That agencies implement segregation of duties between IT functions and Finance functions.

Strategic Planning

An Information Systems strategic plan should be derived from the organisational strategic plan to ensure that appropriate IT functionality is available as required by the organisational plan. Plans should address both short term and long term requirements.

Computer Skills

That agencies specify minimum acceptable levels of IT services, and ensure that resources are adequate to enable those standards to be maintained during periods of leave.

That agencies review the use of external consultants to provide database support, and investigate the possibility of internally providing the functionality.

Personal Computers

That software license registers be upgraded.

That annual inspections of personal computers be performed to check for unlicensed software.

That anti-virus software be installed on all personal computers.

That agencies consider use of startup passwords on personal computers (and particularly portable computers).

INTRODUCTION

Background

This report follows a review of computer environment controls in Government Departments in Tasmania.

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 a component of a comprehensive audit process adopted by audit offices within Australia and overseas.

The project was prompted by the move away by Agencies from a centralised financial system, and implementation of new accounting systems, from 1 July 1996. The previous centralised financial system included strong computer environment controls. With the devolution in responsibility for the new systems there was considered to be a risk of serious weaknesses in computer controls.

However, rather than concentrating exclusively on accounting systems it was determined that the project should focus on departmental information technology sections, thus including coverage of other important systems including human resources, corporate databases, operations support, and property and taxation databases.

The information contained in this report was primarily obtained from a questionnaire completed by each of the information technology section managers in the targeted departments, supplemented by follow up interviews with the managers. Limited field testing was carried out.

Audit appreciates the co-operation and assistance provided by the management and information technology section staff of the departments.

The recommendations made in this report are provided for the information of Heads of Agencies, departmental managers, information technology managers and staff.

Each Head of Agency was provided with a detailed report on audit findings with respect to their agency. Audit will follow up the recommendations in respect to each agency, where appropriate, during the next audit cycle. Some Agencies have already acted on the recommendations made in this report.

Audit Objective

Assess the adequacy of general environmental computer controls in Agencies, whether Agencies have adequate Disaster Recovery Plans and to review software licensing arrangements.

Audit Resources and Timing

The project was initiated in August 1996 and questionnaires issued. Field testing was completed in the period November 1996 to April 1997.

The total cost of the report including the cost of Tasmanian Audit Office staff is estimated at $28 440.00.

Project Methodology

Departments were requested to respond to a questionnaire on computer environment controls. Subsequently, a follow up interview was held between Audit officers and IT Managers to review and verify the responses.

Responses were then entered to a database and analysed.

Scope of the Audit

The agencies selected for review were:

- Department of Community and Health Services
- Department of Transport

- Department of Education, Community and Cultural Development
- Department of Vocational Education and Training
- Department of Environment and Land Management
- Department of Justice
- Department of Police and Public Safety
- Department of Premier and Cabinet
- Department of Premier and Cabinet - Communications and Computing Division
- Department of Primary Industries and Fisheries
- Department of Treasury and Finance
- Tasmania Development and Resources
- Tourism Tasmania
- Parliament:
    - House of Assembly
    - Legislative Council
    - Legislature General
- Tasmanian Audit Office

FINDINGS

Physical Security

Physical security is necessary to ensure the continuity of the installation by protecting the main computer assets and data from accidental or malicious damage, theft or unauthorised use. Ideally access to major hardware should be restricted to operations staff.

Controls	Yes	No	N/A
Access to major hardware (minis, maxis) is restricted to operations staff by locks, cards etc.	14	1	0
The computer room is secured overnight.	15	0	0
There are CIS staff in the area with a view of the computer equipment at all times during the day.	11	3	1

Conclusion

On the basis of the findings from the questionnaire and observation access security was satisfactory at all agencies surveyed.

Protection from Natural Hazards

Protection should exist against fire, flooding, smoke, temperature extremes, power fluctuations, and viruses.

Controls	Yes	No	N/A
There is an adequate device to detect and prevent damage from smoke or heat, (e.g. humidity air conditioners).	11	4	0
There is an adequate device to detect and prevent damage from power fluctuations - power conditioner or uninterrupted power supply.	12	3	0
There are adequate devices to detect and prevent fire damage.	12	3	0
There is a mechanism to prevent water damage - eg. raised platform for computer, drains.	7	7	1

Conclusion

It was noted that half of the agencies surveyed considered that there was a risk of serious water damage. In most instances this was related to the presence of overhead sprinklers, or toilet facilities in the floor above. It was also noted that some agencies did not consider physical security was adequate to prevent damage from power fluctuations, fire or excess smoke and heat.

Recommendation

Agencies should take action to minimise the risks.

Security over Access to the Installation

An access control mechanism associates with identified, authorised users the resources they are permitted to access. Typically access security operates at two levels - access to the installation's operating system, and access to specific computer applications on the installation. This review was concerned only with access to the operating system.

In practice access controls over the installation may be provided by the installation, or by the network through which users access the installation, or by a combination of the installation and the network.

Controls	Yes	No	N/A
All users have a unique ID and password (in contrast to functional passwords where a single password gives many users access to a function).	15	0	0
Access to the operating system is restricted to specific IT staff. All other users are transferred directly to applications which do not allow access to the operating system.	15	0	0
Only a limited number of password attempts are allowed before the system administrator is needed to reinstate the user. (It is not sufficient that the user must log in to the computer again.)	10	5	0
Regular password change is enforced by the installation - the maximum life of a password will depend on the users' access rights.	13	2	0
There is an effectively promulgated security policy - it should be issued to users at least annually.	6	9	0
The system immediately reports security violations to the security administrator.	9	6	0
Minimum length password is enforced - audit recommends at least 6 characters preferably with an enforced mix of alphabetic and numerical characters.	12	3	0
The password file is encrypted.	15	0	0
Previous passwords are stored to prevent re-use of recent passwords. For example the system will not allow the user to alternate between two passwords.	10	5	0
A mechanism exists to ensure that access rights remain relevant - typically a periodic review or a fortnightly report from the Human Resources section of terminated employees.	12	3	0
Computer sessions are automatically logged out if not used for a period (5 - 10 minutes).	7	6	2

Conclusion

It is impossible to evaluate access controls in terms of individual controls. For instance, failure to effectively promulgate a security policy can lead to a poor security culture, so that good computer controls are undermined by failure to keep passwords secret. Similarly the omission of some of the above controls does not necessarily indicate that access control is weak.

Instead, each agency has been assigned a rating based on the following criteria:

- The importance of the data to be protected,
- The presence of the more critical controls,
- An effectively promulgated security policy,
- Restriction on the number of incorrect password guesses allowed,
- Enforced regular change of password,
- Regular review of access rights, and.
- The presence of other security controls.

Results were as follows.

Excellent	Good	Weak	Poor
4	3	4	4

Recommendation

Agencies should develop a security policy, and distribute copies to all staff annually.

Agencies should implement the listed computer controls, and in particular the more important controls:

- Restriction on the number of incorrect password guesses allowed,
- Enforced regular change of password, and
- Regular review of access rights.

Network Security

The development of computer networks has massively increased the power of computers by providing the capacity to share information across networks. However, Network access is inherently less secure than terminal access because there is no need for the user to gain access to terminals. Accordingly the increased functionality has been accompanied by increased risk of illegal access to computer systems, alteration of data and leaking of confidential information.

Experts consider that is that it is impossible to completely secure a network. However, there are some basic steps which should be applied to make networks as secure as possible.

- A firewall is a separate computer which receives all external messages, and forwards communications on to the protected computer after validation.
- Encryption ensures that communications are unintelligible while in transit.
- Limiting of trusted access and other access ensures that gaining access to one computer on the network does not provide automatic access to other computers or data on the network.

Controls	Yes	No	N/A
Use of a firewall between the internal and external networks.	12	3	0
Encryption of networked data.	0	15	0
Limiting the host machines that may look at the file system.	15	0	0
Trusted access is not allowed to other machines.	15	0	0

Conclusion

Firewalls have been implemented in two ways. All departments are connected to external networks through a firewall at the Computing and Communications Division of the Department of Premier and Cabinet. There is also an internal network connecting the government departments and there have been recent attempts to illegally gain access to computer systems by users on the internal network. Most agencies use routers to filter for valid computer addresses. This approach provides most of the functionality of a firewall.

All agencies had appropriate restrictions to prevent their computers or data being accessed by other computers on the network.

Encryption is not currently being used on departmental networks because of the costs involved and performance issues. Departments are accordingly open to the risk that confidential data or passwords could be illegally read off the network.

Recommendation

That agencies periodically review the cost and practicality of implementing encryption on networks.

Dial Up Access

Dial-up and network access is less secure than terminal access. Accordingly one of the following additional security measures should be installed:

- Dial-back facility,
- Password on the modem,
- Receiving modem is normally disabled except when required.

Control	Yes	No	N/A
Dial-up access where available includes a dial back procedure, a dial up password or other protection.	12	2	1

Conclusion

All agencies either had an additional security measure, or were currently investigating such security measures.

Backup of Information

Information is an important asset of any organisation and particularly government agencies. Computerised storage of information provides increased risk that data can be deleted, overwritten or corrupted. Accordingly it is important that information be backed up regularly, verified and placed in a secure location.

Controls	Yes	No	N/A
Backup is regularly performed at intervals appropriate to the amount of input and the sensitivity of the application	15	0	0
System software, application software, and data are backed up.	15	0	0
A tape cycle is used that ensures that annual, monthly and daily backup is available.	15	0	0
Where appropriate a vendor recommended method of backup is used (eg. Checkpointing in CA-Ingres).	14	1	0
Backup is regularly stored off site at intervals appropriate to the amount of input and the sensitivity of the application	14	1	0
Backup tapes are periodically tested.	10	5	0
Backup tapes are regularly replaced in accordance with manufacturer recommendations.	12	3	0

Conclusion

Backup of information is generally reliable although it was noted that one agency did not store its backups in an off-site location. Backups need to be periodically tested to ensure that the tapes can be read as required, and it was noted that a third of the agencies surveyed did not perform such testing.

Recommendation

There should be a process of testing tapes to ensure that the backup process is effective and that tapes can be read.

Disaster Recovery Plan

With the increasing focus on the use of computers in Agencies it is becoming more critical as part of an Agencies business continuity plans that as a matter of priority every Agency should have a disaster recovery plan.

A disaster recovery plan documents detailed recovery procedures to restore an organisations processing capabilities, within a specified time frame, in the event some form of disaster makes the computer facility inoperable and threatens important operations within the Agency.

The plan should include:

- Backup strategies for hardware, software, data communications, and key personnel,
- Determination of critical systems for the agency and estimates of costs and the period for which it is acceptable to be without those systems,
- Determination of risks to the computer facility, and strategies for minimising those risks,
- Detailed procedures and identification of the officers to perform the procedures, and
- A detailed testing strategy to ensure the plan will be effective if required.

Audit noted that none of the agencies surveyed had a completed disaster recovery plan, although three agencies had draft (untested) plans, and most other agencies were planning to develop a disaster recovery plan within the next two years.

Recommendation

That all agencies give priority to development of a disaster recovery plan.

Recovery from System Failure

Data may be at risk when a system failure occurs because of the presence of partially completed transactions. At best these represent errors in the system, at worst an entire database can become corrupted. A mechanism should exist to ensure that restarts and recoveries are properly performed, authorised and logged.

Controls	Yes	No	N/A
The computer facility has proven recovery procedures	14	0	1
All system failures and recovery actions are documented in an incident diary.	10	4	1
There is clear documentation of procedures for recovering after a system failure.	8	6	1

Conclusion

The use of database systems with proven recovery procedures, provides a reasonable level of control over the risk, however the lack of incident diaries, and documentation of recovery procedures at a number of agencies is of concern.

Recommendations

That agencies implement incident diaries.

That agencies write recovery procedures for all major systems.

Data Editors

Ideally data should only be edited through application menu options to ensure that audit trails are created, and

that controls over input of data are not bypassed.

However, it is sometimes necessary to edit data directly rather than using application menu options, for example, after a system failure, or to correct errors caused by a program fault.

It is essential that the changes:

- are authorised by the person responsible for the data (for example. the accountant), and
- are recorded on the original audit trails and transaction reports, or in a separate register.

Controls	Yes	No	N/A
Access to data editors (eg SQL) is restricted to persons with appropriate skills and seniority (e.g. system administrator)	11	2	2
Use of direct editing of data must be approved by the owner of the system (eg. Finance Manager).	9	3	3
Each direct edit and the reason it was considered necessary are documented.	8	2	5
Where direct editing is used 'before images' and 'after' images are retained.	5	5	5

Conclusion

The following problems were noted:

- One Finance Manager was also the officer in charge of the IT section. This was considered necessary because of the small size of the corporate services section.
- One senior finance officer had been given access to the data because of his IT skills to develop reports and other minor processes.
- Important databases had been developed externally to IT sections, and were not subject to the standards applied in the IT section.
- Documentation of edits was seen to be the responsibility of the owners of the data, rather than the IT section.

Recommendations

That agencies implement segregation of duties between IT functions and Finance functions.

That as far as possible data should only be edited through application menu options.

That where it is necessary to use direct editing of data, appropriate approval and documentation standards be applied.

Change Control

Changes to software may be needed to improve performance (upgrades) or to correct faults (patches). However, implementation of the changes creates some significant risks:

- Data can be corrupted or lost because of faulty software,
- The software may no longer process data correctly.

Accordingly, a formal change process is needed to ensure that only tested and authorised changes are made.

Controls	Yes	No	N/A
There are formal procedures (including sign off) for implementing new software / upgrades / patches.	8	5	2

Formal procedures exist for testing new versions and upgrades.	10	3	2
Formal procedures exist for testing patches.	9	4	2
There is a systematic testing approach possibly including use of standard test data.	9	4	2
There is a test environment for testing new software.	14	0	1

Conclusion

A number of agencies lacked formal processes in this area. This particularly applied to new finance systems, where external consultants had made changes to production versions of software without formal approval processes.

Recommendations

That agencies implement formal processes over change control for important applications.

Segregation of Duties

Many accounting controls rely on staff only being allowed to access specified functions in accounting systems. IT staff typically have the power to set access rights for themselves and others, as well as having direct access to the data, and accordingly have the capacity to bypass many of the accounting controls. To some extent this is an unavoidable weakness, however the weakness can be minimised by ensuring a clear segregation of duties between accounting staff and IT staff.

Controls	Yes	No	N/A
Accounting staff do not have access to IT functions (e.g. data administration).	12	2	1
IT personnel do not have write access to finance systems.	13	2	1

Conclusion

Three separate problems were noted:

- One Finance Manager was also the officer in charge of the IT section. This was considered necessary because of the small size of the corporate services section.
- One senior finance officer had been given access to the data because of his IT skills to develop reports and other minor processes.
- Two IT officers were required to provide occasional support to the finance section.

Recommendation

That agencies implement segregation of duties between IT functions and Finance functions.

Strategic Planning

An Information Systems strategic plan should be derived from the organisational strategic plan to ensure that appropriate IT functionality is available as required by the organisational plan. Plans should address both short term and long term requirements.

Controls	Yes	No	N/A
There is a strategic plan for information technology which is consistent	10	4	1

with corporate goals.			
There are short term and long term plans for information technology.	12	3	0

Conclusion

In some instances there was no current strategic/corporate plan for the organisation, and as a consequence no strategic plan. All agencies with a corporate plan either had an IT strategic plan, or were currently developing a plan.

Computer Skills

Controls	Yes	No	N/A
The IT section includes people with adequate qualifications/experience in IT management.	15	0	0
The IT section includes people with adequate qualifications/experience in IT administration.	15	0	0
The IT section includes people with adequate qualifications/experience in networking.	15	0	0
The IT section includes people with adequate qualifications/experience in programming and analysis.	14	0	1
There are adequate arrangements to ensure skill level maintained during periods of staff leave.	10	5	0

Conclusion

All agencies surveyed were satisfied with their current skill level. However, some agencies expressed concern about their capacity to maintain the normal standard of IT services during periods of leave.

It was also noted that some agencies were relying on external consultants for report writing, data extraction and other database functions for the Finance system. Whether this was because of a reluctance by Finance sections to use their IT Sections, or a lack of relational database skills, Audit is concerned that agencies may not be fully utilising the software, and/or may be incurring unnecessary expense.

Recommendation

That agencies specify minimum acceptable levels of IT services, and ensure that resources are adequate to enable those standards to be maintained during periods of leave.

That agencies review the use of external consultants to provide database support, and investigate the possibility of internally providing the functionality.

Personal Computers

Some risks inherent to personal computers are as follows:

- Physical access is unrestricted,
- Logical access controls are typically weak or non-existent,
- Data is not automatically backed up.
- It is important that control exists over loading and running of software on computers, whether that be on mainframes or Personal Computers. Agencies should ensure that only licensed software is being used on their systems.
- The possibility exists for Agencies to face large fines if they are found to have installed software on more machines than the user's license permits, or to be using unlicensed software. The proper use of a software register and the periodical audit of the software should be considered by management as part of its normal internal controls.
- There is less control over installation of software, which allows the possibility that an organisation might be embarrassed by a software audit.

The risks can be reduced by implementation of the following controls.

Controls	Yes	No	N/A
New versions of anti virus software are installed on all personal computers.	11	4	0
All installed software is licensed.	15	0	0
A register of licenses is maintained for all software (PCs and other computers).	12	3	0
Periodic inspections of PCs are carried out to check for unauthorised software.	5	10	0
Registration payments are made for all shareware software in accordance with the software conditions.	13	0	2
A startup password is required for all personal computers.	6	9	0

Conclusion

There is a significant risk that unlicensed software may exist on personal computers because of:

- Failure to maintain software license registers (registers did not exist at three agencies, and were poorly maintained at most other agencies),
- Periodic inspections are not performed, so that unlicensed software may be installed by users without detection.

It was noted that four agencies did not install anti-virus software on their computers allowing the possibility of loss or corruption of data on their computers, and on network file servers.

Security over confidential data on personal computers may be at risk because of the absence of startup passwords on personal computers.

Recommendations

That software license registers be upgraded.

That annual inspections of personal computers be performed to check for unlicensed software.

That anti-virus software be installed on all personal computers.

That agencies consider use of startup passwords on personal computers (and particularly portable computers).

Audit Opinion

This audit has been performed in accordance with Australian Auditing Standards AUS 806 Performance Auditing.

The standard states 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 or entities' activities have been carried out economically, and/or efficiently and/or effectively.

Because of the nature of this audit and the across Agency approach, I do not believe it is possible to provide an opinion in the terms set out above.

However, the audit identified that across all Agencies there is a need for overall improvement in general environmental computer controls together with priority given to the introduction of, or testing of, disaster recovery plans.

PREVIOUS REPORTS TO PARLIAMENT

1992	**SPECIAL REPORT NO. 1**	**REGIONAL HEALTH SUPPORT SERVICES**
1992	**SPECIAL REPORT NO. 2**	**STUDENT TRANSPORT**
1993	**SPECIAL REPORT NO. 3**	**EDUCATION INSTITUTIONS CLEANING SERVICES**
1993	**SPECIAL REPORT NO. 4**	**STANDARD OF ANNUAL REPORTING BY GOVERNMENT DEPARTMENTS**
1993	**SPECIAL REPORT NO. 5**	**MUNICIPAL SOLID WASTE MANAGEMENT**
1994	**SPECIAL REPORT NO. 6**	**ADMINISTRATION AND ACCOUNTABILITY OF GRANTS**
1994	**SPECIAL REPORT NO. 7**	**REGIONAL HEALTH MEDICAL REVIEW**
1994	**SPECIAL REPORT NO. 8**	**WASTEWATER MANAGEMENT IN LOCAL GOVERNMENT**
1995	**SPECIAL REPORT NO. 9**	**HERITAGE COLLECTION MANAGEMENT**
1995	**SPECIAL REPORT NO. 10**	**OFFICE ACCOMMODATION MANAGEMENT**
1995	**SPECIAL REPORT NO. 11**	**RECORDING AND REPORTING BY GOVERNMENT DEPARTMENTS OF THEIR NON-CURRENT PHYSICAL ASSETS**
1995	**SPECIAL REPORT NO. 12**	**TENDERED WORKS**
1996	**SPECIAL REPORT NO. 13**	**NURSING COSTS IN TASMANIA**
1996	**SPECIAL REPORT NO. 14**	**REVIEW OF PERFORMANCE INDICATORS IN GOVERNMENT DEPARTMENTS**
1996	**SPECIAL REPORT NO. 15**	**CASH MANAGEMENT IN LOCAL GOVERNMENT**
1996	**SPECIAL REPORT NO. 16**	**DEPARTMENTAL ACCOUNTING MANUALS AND COMPLIANCE WITH PROCEDURES**
1997	**SPECIAL REPORT NO. 17**	**AIR TRAVEL**
1997	**SPECIAL REPORT NO. 18**	**ADMINISTRATION OF STATE GOVERNMENT CONCESSIONS**
1997	**SPECIAL REPORT NO. 19**	**COMPLIANCE WITH SUPERANNUATION GUARANTEE ARRANGEMENTS**