[P.P.4B

S O U T H A U S T R A L I A

———————————————————

Report

of the

Auditor-General

for the

Year ended 30 June 2003

———————————————————————————————

Tabled in the House of Assembly and ordered to be published, 4 December 2003

———————————————————————————————

Third Session, Fiftieth Parliament

Supplementary Report

Information and Communications Technology – Future Directions: Management and Control

By Authority: J. D. Ferguson, Government Printer, South Australia

2003

Government
of South Australia

Auditor-General's Department

Auditor-General's Department
9th Floor State Administration Centre
200 Victoria Square
Adelaide
South Australia 5000

Telephone +61 +8 8226 9640
Facsimile +61 +8 8226 9688
DX 56208 Victoria Square

E-mail: admin@audit.sa.gov.au
Web: http://www.audit.sa.gov.au

ABN: 53 327 061 410

3 December 2003

The Hon R R Roberts, MLC
President
Legislative Council
Parliament House
ADELAIDE SA 5000

The Hon I P Lewis, MP
Speaker
House of Assembly
Parliament House
ADELAIDE SA 5000

Gentlemen,

AUDITOR-GENERAL'S SUPPLEMENTARY REPORT: INFORMATION AND COMMUNICATIONS TECHNOLOGY – FUTURE DIRECTIONS: MANAGEMENT AND CONTROL

Pursuant to section 36(3) of the *Public Finance and Audit Act 1987*, I herewith provide to each of you a copy of my Supplementary Report 'Information and Communications Technology – Future Directions: Management and Control'.

Yours sincerely,

K I MacPherson
AUDITOR-GENERAL

Supplementary Report of the Auditor-General 2002-03

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

Supplementary Report of the Auditor-General 2002-03

TABLE OF CONTENTS

Supplementary Report of the Auditor-General 2002-03

TABLE OF CONTENTS

Supplementary Report of the Auditor-General 2002-03

TABLE OF CONTENTS

GLOSSARY

AGENCY SYSTEM REFERENCES

CARS	Capture Adjudication and Reporting System
CCMS	Civil Case Management System
CHRIS	Complete Human Resource Information System
Concept	Human Resource Management System (HRMS)
DRIVERS	Driver and Vehicle Registration System
EDSAS	Education Department School Administrative System
GMMS	Gaming Machine Monitoring System
IEPS	Integrated Electronic Purchasing Solution
Oacis	Open Architecture Clinical Information System
RISTEC	RevenueSA Information Systems to Enable Compliance
RPS	Results Processing System
TIMBER	Taxation Information Money By Electronic Return
TRUMPS	Transport User Management Processing System
WILMA	Water Information And Licence Management Administration System

SPECIFIC TERMS

CIO	Chief Information Officer
GPTF	Government Purchasing Task Force
ICT	Information and Communications Technology
ISMF	Information Security Management Framework
MPICC	Major Projects and Infrastructure Cabinet Committee
NPP	National Privacy Principles
PMG	Prudential Management Group

EXECUTIVE SUMMARY

BACKGROUND

Information Technology is a cornerstone in the provision of service to the community in both public and private sectors and is indispensable in supporting government operations and public sector agencies' delivery of services and financial reporting requirements.

The current public sector IT arrangements are characterised by large outsourcing contracts with the private sector. This includes the provision of government IT infrastructure, communications, and radio networks. Those arrangements support key government-wide financial systems for accounts payable, accounts receivable and human resource management systems.

The effective management and the security and control of agency financial and operational systems and IT infrastructure, is important for ensuring the completeness, accuracy and integrity of information. It is this information that underpins financial reporting and operational management decision making.

These systems and services may be referred to collectively as Information and Communication Technology (ICT). The increasing reliance upon ICT to support service delivery and the operations of government gives rise to identifiable risks that require active management in order that the public interest may be protected.

The development, implementation, operation and ongoing management of these systems and services in the context of an endorsed strategy and direction for the State is a significant management and technical task.

For the reasons discussed in this Report, with respect to ICT matters, there are a number of areas of central government and agency management and operations that are in need of improvement. A number of these matters have been the subject of Audit commentary in earlier Reports to Parliament.

Audit Mandate

The Audit review process was conducted pursuant to section 36 of the *Public Finance and Audit Act 1987.*

Pursuant to the *Public Finance and Audit Act 1987* the Auditor-General is required to form and express certain opinions in relation to each agency of government that is subject to audit by the Auditor-General. Those opinions relate to the integrity of the financial statements prepared by each agency and the controls exercised by each agency over their respective financial transactions and assets.

The management, security and control of IT infrastructure and systems is essential for the completeness, accuracy and integrity of financial record keeping and the production of financial statements as well as the achievement of government and agency operational objectives. Effective management in these matters is essential for the ongoing continuity and control of business operations and the protection of agencies information and assets.

DAIS has important responsibilities for the planning, leadership and direction of major Government IT initiatives and IT infrastructure, including government-wide systems and

information and communications technology use. Individual agencies in their own right are also responsible for the development of a significant range of diverse systems. These systems deal with a number of major areas of government service delivery and financial operations.

It is within this context and having regard to the public interest importance of IT in governmental operations that the reviews included in this Report have been undertaken.

PAST AUDIT OBSERVATIONS

My Reports for the last few years have stressed the need to address some inadequacies concerning the controls associated with IT governance and management both at a central agency and individual agency level. I have also commented on the need for improvement in critical whole-of-government and agency security control policy, standards and procedures, and, arrangements for ongoing continuity of operations.

Broadly speaking, I have related the need for improvement in central agency strategy, policy, direction, planning and monitoring, and on security control of agency systems and facilities, and project and risk management arrangements. I have also provided comment on certain legal and management aspects of e-government operations through the review of a number of selected agency e-commerce reviews, mainly involving contracts with the private sector.

One particular matter subject to comment over the past few years has been the need for finalisation and communication of a government IT Plan. In that regard, I commented that planned significant projects and the necessary actions to be initiated by government and its agencies regarding the management of those projects need to be identified, prioritised, and monitored. The monitoring and regular reporting to Executive Government (Cabinet)[1] should be undertaken by the Senior Management Council, Department for Administrative and Information Services (DAIS) and the relevant agencies. Each of these matters is dealt with in this Report.

RECENT GOVERNMENT DEVELOPMENTS

The latter part of 2002 and into 2003 has seen certain initiatives taken by DAIS in recognition of the requirement for improvement in ICT governance and management.

The separate initiatives that were outlined in a number of Cabinet submissions, addressed the need for a consolidated approach to ICT across government and the increased involvement by senior agency management in the planning and management of ICT as a shared resource.

The initiatives have resulted in the strengthening of ICT governance and management arrangements notably the:

- broadening of the role and responsibilities of the Major Projects and Infrastructure Cabinet Committee to include consideration of ICT strategy, policy and standards and, ICT sourcing arrangements;

---

[1] In this Report references to the 'Executive Government' are intended to refer to the 'Cabinet'. These terms are used interchangeably throughout this Report depending upon the context. This has been done to assist in understanding the process associated with certain matters.

- establishment of the ICT Strategy, Policy, and Standards Steering Committee.
- establishment of the Future ICT Service Arrangements Steering Committee.

The latter initiative forms part of the overall arrangements being implemented to focus on the future IT acquisition and services program of government.

In conjunction with the establishment of revised governance initiatives, DAIS has undertaken the redevelopment of the government ICT strategy and aspects of ICT policy standards revision.

AUDIT FOCUS 2002 and 2003

During 2002 and 2003, Audit has maintained a focus on IT Governance and Management Control matters at a whole-of-government and agency level and has undertaken a number of specific reviews.

This Report, comprising four Parts, deals specifically with Audit's review of certain aspects of government and agency operations relating to:

- IT Governance and Management;
- Project and Risk Management for Major IT Developments;
- IT Security and Control;
- IT Legal Considerations in Electronic Government.

Fundamental Governance Aspects Examined

The reviews took into consideration matters of a management control nature, that in the opinion of Audit, would ordinarily be regarded as important elements of an overall IT governance framework.

The important elements are described below under key responsibility areas of government.

Executive Government (Cabinet)

Endorsement of an IT vision, a whole-of-government IT Plan, and a framework of IT strategy, policies and standards. Cabinet approval of major projects and ongoing monitoring of the status of major projects.

DAIS (as Lead Agency for IT in conjunction with other Agencies)

Development of IT vision and whole-of-government IT plan, with associated strategy, policy and standards framework; implementation and management of whole-of-government IT projects and management of major government IT contracts. High level monitoring and reporting to Executive Government on the status of major whole-of-government IT projects.

Agencies

Maintenance of an IT strategic plan; establishment of an internal control framework; obtaining Cabinet approval for major IT projects; implementation of project governance and risk management arrangements; regular reporting of major IT project status; and provisions for continuity of business operations.

In the context of the reviews, Audit has formally conveyed the issues that have arisen to the relevant agencies. A response has been received from each of those agencies.

Summarised below are those matters identified by Audit as still requiring resolution, together with some suggestions for improvement. These suggestions have been communicated to DAIS as the lead agency for Information Technology. DAIS's response is included herein.

MATTERS REQUIRING RESOLUTION

Important matters that Audit considers are still in need of resolution are dealt with in the relevant Parts of this Report. The following summarises significant matters that are examined in those Parts.

Part 1 - IT Governance and Management

Planning, Coordination and Monitoring of IT Initiatives and Projects

Part 1 deals with the key governance arrangements for management of Information Technology at a whole-of-government and agency level. It examines recent government developments in this area and identifies some important matters that, in Audit's opinion, require further attention.

Certain initiatives have been taken by government during 2002 and the earlier part of 2003 to strengthen some aspects of ICT governance. This has involved aspects of strategy, policy and standards and the future sourcing of ICT services.

Essentially, the review work completed by Audit has identified certain inadequacies in areas of IT planning, monitoring and reporting of IT initiatives. For example, it is evident at this time, that there is a need for a consolidated whole-of-government IT plan. That plan would significantly facilitate prioritisation and effective monitoring of those projects for reporting to Executive Government.

There have also been inadequacies identified with respect to current policies and standards covering IT operations of government.

The current administrative arrangements, including some recent initiatives that have been taken, in my opinion, do not address sufficiently the requirement for clear responsibility for high level coordination and monitoring of major government approved IT project developments. The consequence of this fact is that the Executive Government may not be provided with advice that would allow, when circumstances so require, for timely remedial steps to be taken to correct and/or prevent a problem.

In my opinion, coordination, monitoring and accountability may be assisted by a centrally managed agency establishing a position of Chief Information Officer who would have appropriate authority and who would have a whole-of-government perspective.

It is of interest that, in a Report in 2000 under the title, 'Governance and Oversight of Large Information Technology Projects', the Controller and Auditor-General of New Zealand noted:

- *Central agencies have clearly defined roles in monitoring the development of business cases and the progress of projects. The Minister should expect sound advice from them on these matters.*

- *The Select Committees role is one of strategic oversight and high level accountability. The oversight and accountability processes of Select Committees can be extremely influential and may impact strongly on the project.*

- *Treasury and (central agency) officials are accountable to their Ministers to provide correct and complete advice about the viability of the business case, to monitor project progress against benchmarks, and to alert Ministers promptly when a project gets into trouble.*

One would not expect the situation to be different in the South Australian jurisdiction.

Audit Suggestions for Improvement

In August and October 2003, Audit formally communicated to DAIS (as Lead Agency for IT) certain suggestions for improvement with respect to overall IT Governance and Management arrangements. The matters contained in two management letters have been discussed with the management of DAIS.

DAIS has responded in a detailed manner to the two management letters.

In its responses, DAIS recognised that further improvement, beyond the initiatives taken in 2002 and 2003, was required in a number of areas of ICT governance at a whole-of-government and agency level. Specifically, DAIS recognised Audit's concerns in relation to the high-level monitoring and consolidated reporting of ICT status in the South Australian public sector. DAIS provided advice on a series of initiatives that were under consideration that would significantly address the matters raised by Audit.

As many of the matters to be addressed are at a whole-of-government, as well as agency level, DAIS indicated that this will require considerable engagement with agencies and other key stakeholders in developing and agreeing a formal program of work in respect to the initiatives under consideration.

Overall, the initiatives consider areas of leadership in ICT; ICT planning; ICT investment and prioritisation; ICT policy; ICT monitoring and control; and ICT coordination and compliance.

It is not, however, clear as to whether the initiatives would include the measurement and reporting of the status of Cabinet approved IT projects against a consolidated IT plan of Cabinet expectations. Adoption of the initiatives would involve consideration at an Executive Government level.

DAIS intends that the detailed work plan and proposals associated with the initiatives under consideration be developed in collaboration with the key relevant agencies and management groups across government. It is planned that the initiatives will be the subject of a Cabinet submission in the March quarter of 2004.

These matters are commented on in more detail in Part 1 of this Report.

Part 2 - Project and Risk Management for Major IT Developments

Audit Reviews of Major Projects

Part 2 examines some major IT project developments of the Government and its agencies. There are a number of well documented cases within Australia and internationally of large IT project developments running into major problems, and in some cases failing completely. The developments examined in this Part of this Report

give an insight into problems encountered by certain agencies in this State in the management of major IT projects. It also highlights some areas that, in my opinion, require remedial action.

Audit has reviewed the procurement area of electronic commerce managed by DAIS. Audit has also reviewed, from a whole-of-government perspective, the Human Resource Management system (CHRIS) and the DECS Human Resource Management System replacement.

The sensitive area of medical information has been addressed with the review of the 'Oacis' programme of the Department of Human Services. Other projects selected for this review include agency electronic commerce facilities and web sites for financial transaction processing. These mainly relate to motor vehicle and driver licences, the electronic lodgement of court claims, and the revenue raising area of taxation.

In addition, Audit has reviewed new system developments for the Water, Land and Biodiversity Conservation agency.

Key IT related control requirements which must be met by agencies are, inter alia, contained in the Financial Management Framework and Treasurer's Instructions issued by the Department of Treasury and Finance and guidance from the Prudential Management Group.

Weaknesses found in some of the IT project developments examined, were:

- project delays and extended timeframes for completion;
- lack of advice of significant change in status of projects and/or the failure to provide periodic status reports to Cabinet or the Prudential Management Group;
- inadequacies in agencies' risk and project management arrangements when outsourcing with the private sector;
- inadequate recording/monitoring of project costs and benefits;
- risk management arrangements not revisited on a regular basis as may be necessary.

The failure to adequately manage the issues identified can result in the incurring of substantially increased costs in the delivery of project outcomes.

Audit Suggestions for Improvement

The matters identified by Audit have been formally communicated to, and discussed with, the agencies and with DAIS. As part of that process, Audit submitted certain suggestions for improvement. Responses have been received from all agencies and from DAIS.

In Audit's opinion, where problems have been encountered they stem broadly from certain inadequacies in agency planning, project monitoring, reporting, and risk management arrangements.

Audit considered that these areas could be improved by agencies ensuring that certain antecedents were in place prior to submitting IT project proposals to Cabinet for approval. These would include:

- agency business plans and approved IT strategic plans;
- implementation plan for the project, including periodic update status provision to Cabinet;
- evidence of appropriate project and risk management governance skills and processes.

To assist with monitoring and reporting, individual agency Chief Information Officers should report progress and status of all major approved agency IT initiatives to the agency Chief Executive and to Cabinet. Reporting could/would be in accordance with implementation plan requirements as advised in initial Cabinet submissions.

More detailed commentary in respect of these reviews is presented in this Part of this Report.

Part 3 - IT Security and Control

Audit Reviews of IT Systems and Computing Environment

Part 3 examines Audit's reviews of key aspects of agency IT Security and Control. The Auditor-General's Department audits in excess of 160 public sector entities, including administrative agencies of government, health units, and other public sector entities.

This Part specifically addresses the reviews undertaken in respect to IT systems, facilities, and operations, at a selected number of those entities. The matters addressed relate to matters concerning strategic and business continuity planning; day to day operating procedures; arrangements with the private sector; access to systems and information; and implementation and maintenance of systems and facilities.

The reviews of systems and their supporting computing environments have been undertaken against the Government mandated security control requirements promulgated in December 1994, as supplemented by more current better practice procedures in management and control of IT systems and facilities.

Audit identified notable weaknesses in agencies' security arrangements, including:

- inadequate attention to strategic management and planning for IT;
- weaknesses in access provided to users to systems and information;
- unsatisfactory contract agreements with the private sector for IT service provision;
- need for improvement in documented security and operational policies and procedures;
- lack of current documented and tested business continuity arrangements.

New standards are being introduced by government to address the current requirements of information security. This is being done through the promulgation of a new Information Security Management Framework. It is also proposed to have a formal education program to ensure that all agencies are fully aware of the new standards and how to apply them.

Audit Suggestions for Improvement

The matters identified in the reviews have been formally communicated to and discussed with the agencies and with DAIS. As part of that process, Audit submitted certain suggestions for improvement. Responses have been received from all agencies and DAIS.

The effective management, security and control of agency systems and computer processing environments is essential for the completeness, accuracy and integrity of financial record keeping and financial statement production as well as the achievement of government and agency operational objectives. These management and security control arrangements are essential components for the ongoing continuity of business operations and the protection of agencies information and assets.

These matters are commented on in more detail in Part 3 of this Report.

Part 4 - IT Legal Considerations in Electronic Government

Legal Issues and Risks

The final Part of this Report presents the findings of further work completed by Audit during 2002 and 2003 in revisiting the legislative framework for electronic government, and the review of some major electronic commerce and web site facility developments of government agencies.

Audit's reviews focused on matters of a legal and contract nature and aspects of risk management in selected government agencies. The reviews also addressed agency Web site facilities for compliance with government requirements and better practice management.

This Part identifies certain legal matters and risks evident in government and agency management of electronic government initiatives and management and control of web site facilities and information. These matters include the following:

- inherent limitations in the operation of the *Electronic Transactions Act 2000* (SA).
- Inadequacies in agencies' risk management arrangements when outsourcing electronic initiatives with the private sector and the risk of inaccurate data entry and breaches by third parties.
- Intellectual property rights not in all case, being properly documented.
- Government and agency web site disclaimers are considered inadequate for some key agencies.

This Part also comments on the potential to consider the importance and benefits of establishing a legislative basis for the operation of privacy principles for State Government agencies.

Audit Suggestions for Improvement

Legal matters and risks arising from Audit's review of the legislative framework and selected agency electronic commerce and web site facility developments were communicated and discussed with the relevant agencies, including DAIS.

Those communications included certain suggestions to address the matters raised by Audit, both at an agency and whole-of-government level.

The specific issues are more fully examined in this Part of this Report.

PART 1 — IT GOVERNANCE AND MANAGEMENT

PART 1 — IT GOVERNANCE AND MANAGEMENT

TABLE OF CONTENTS

CHAPTER 1 — REVIEW BACKGROUND AND KEY AUDIT FINDINGS AND COMMENTS

BACKGROUND

Introduction

This Part of the Report examines some of the key governance arrangements for the management and control of Information and Communications Technologies at both the whole-of-government level and with respect to several major public sector agencies.

DAIS has important responsibilities within government in the areas of strategy, policy, planning, and the management of government-wide IT initiatives and operations. DAIS carries out its responsibilities, inter alia within the parameters established by its responsible Minister and by Cabinet. Individual agencies also have their own responsibilities in relation to IT matters and some agencies undertake significant IT initiatives in their own right. In the latter case, these matters are undertaken, inter alia, in accordance with the requirements of the responsible Minister and, in some instances, as may be established by Cabinet.

During 2002 and 2003, Audit has undertaken reviews of several areas of IT management and operations. Matters that have arisen in the course of these reviews are reported upon in this Report.

Audit Mandate

The Audit review process was conducted pursuant to section 36 of the *Public Finance and Audit Act 1987.*

Past Audit Observations

My Reports to Parliament (Part A) for the last few years have emphasised the importance of key aspects of whole-of-government IT Governance and Management Control (strategic planning, policy and guidance to agencies), and the need to address identified inadequacies. Reports during this period have also included comment on the need for improvement in agency security control matters, ie agency systems and computer processing environments including business recovery arrangements.[2]

One important matter subject to comment over the past few years has been the need for finalisation of a public sector IT Plan. Further, Audit has commented that planned projects need to be prioritised, developed, and monitored by the Senior Management Council, DAIS and the agencies. [3]

Furthermore, I also commented that the IT Policy and Standards framework of DAIS required revisiting. This is particularly the case having regard to the changing technological environment and developing codes of practice in Information Technology. The emerging significance of e-commerce generally is a matter of particular interest in this context.

---

2 Specifically, I have related the need for improvement in coordination and control at a central agency level ie strategy, policy, security control of agency systems and facilities, risk and project management arrangements, certain legal aspects of e-government operations, and business continuity planning at a government-wide and agency level.

3 Report of the Auditor-General year ended 30 June 2001, Part A - Audit Overview, p 136.

These matters have been subject to formal communications to DAIS over the past few years and in past Reports to the Parliament.

Audit Review Focus - 2002 and 2003

During 2002 and 2003, Audit has maintained a focus on IT governance and management control, at a government-wide and individual agency level. In particular, Audit has:

- reviewed the strategy, policy, standards, and planning, monitoring and reporting of IT initiatives and operations;
- undertaken a review of the project and risk management processes and achievements of some major IT developments of selected agencies;
- reviewed the controls over other major financial and information systems. This has included computer processing environments of agencies covering the education, health and justice sectors, and the revenue raising, and gaming areas of Government operations;
- examined matters of a legal and contract nature related to a number of IT developments of key agencies.

RECENT GOVERNMENT DEVELOPMENTS

During the latter part of 2002 and extending into 2003, certain initiatives have been taken by DAIS in recognition of the requirement for improvement in ICT governance and management.

These initiatives addressed the need for a consolidated approach to ICT across government and the need for the increased involvement by senior agency management in the planning and management of ICT as a shared resource.

These initiatives have resulted in the strengthening of ICT governance and management arrangements, notably the:

- broadening of the role and responsibilities of the Major Projects and Infrastructure Cabinet Committee (MPICC) to include consideration of ICT strategy, policy, standards, and, ICT sourcing arrangements;
- establishment of the ICT Strategy, Policy and Standards Steering Committee;
- establishment of the Future ICT Service Arrangements Steering Committee.

The latter initiative forms part of the overall arrangements being implemented to focus on the future IT acquisition and services program of government.

In conjunction with the establishment of the revised governance initiatives, DAIS has undertaken the redevelopment of the government ICT strategy. It has also revised aspects of ICT policy and standards. Further brief commentary on these developments follows.

ICT Directions Strategy

In August 2003, the Minister for Administrative Services publicly launched a document titled ‘ICT Directions’. This document essentially presents a ‘vision’ document that is intended as guidance for public sector decision makers. It was not intended to be a

whole-of-government IT plan with specific outcomes for major IT developments that could be measured and monitored against government approved expectations.

IT Policy and Standards

As mentioned, an important governance initiative at a government level has been the establishment of the ICT Strategy, Policy and Standards Steering Committee. That Committee, chaired by the Chief Executive of DAIS, has the facilitation of strategies, policies and standards for government ICT as one of its principal responsibilities. These matters are referred to the Major Projects and Infrastructure Cabinet Committee for endorsement.

An important recent outcome concerning policy and standards has been the development and release of the 'Information Security Management Framework'.

Information Security Management Framework

In April 2003, the SA Government Information Security Management Framework (ISMF) was approved as the current Information Technology security standards and guidelines for implementation by agencies.

The ISMF represents an alignment of South Australian public sector arrangements with international information technology security standards. These standards are being adopted by all Australian Governments and provide a basis that will ensure a consistent approach for all South Australian Government agencies in protecting business operations.

The ISMF is yet to be fully implemented. It will be introduced through a program of work including, a transition guide from current standards and guidelines, provision of agency security awareness training, and, the integration of new security work practices. The implementation and operation of the overall security program is estimated to cost in the vicinity of $1.3 million over four years.

The ISMF, replaces the existing standard that was promulgated in 1994, ie Government's 'Information Technology Security Standards - In an Outsourced Environment'.

Each of the abovementioned developments and observations have been taken into consideration in Audit's review process.

GOVERNMENT IT ENVIRONMENT

IT Systems and Infrastructure

Public sector agencies operate in an IT environment characterised by an extensive and diverse range of systems and computing facilities.

Systems that vary widely in complexity operate across the public sector spectrum. Some systems are of major importance and include government-wide Human Resource Management systems, government-wide financial management systems, revenue taxation systems, clinical health care systems, and school based administrative and financial systems.

Systems can also be developed and managed internally or be subject to outsourced service provider arrangements.

The IT Infrastructure of government substantially consists of:

- a number of computing mainframe environments and mid range computing environments located at EDS (Australia) Limited (EDS) processing bureau at Glenside. These computers process major government systems in all areas of governmental operation;

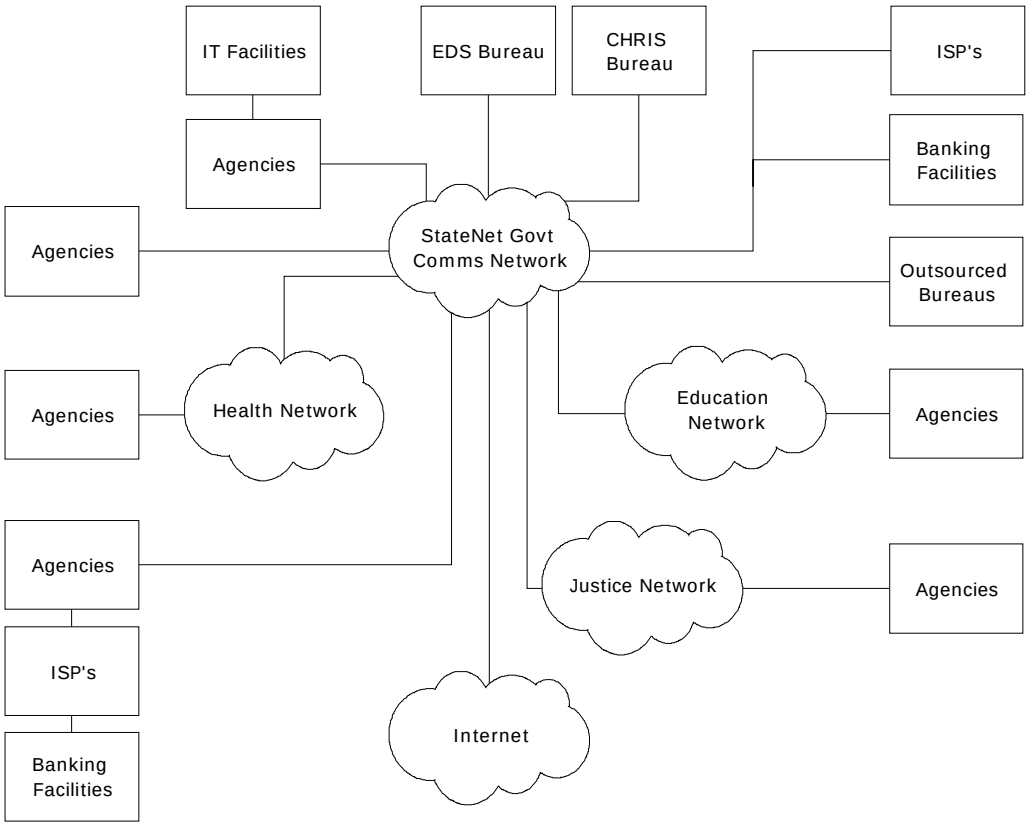
- individual agencies have significant computing environments 'on site' essentially consisting of mid range computers or desk top computers attached to local area networks. These are either under EDS management control or the control of the individual agency;

- many agencies have agreements with private sector service providers for external services. By way of example, these agreements provide for specialised e-commerce and Internet web site facilities, and external bureau service arrangements for payroll and other systems. The private sector service providers in some cases store and process government information on their computing environments.

The majority of agencies are connected to the Government's wide area communication network, StateNet. StateNet provides access to the EDS Glenside Bureau processing facilities and also provides a 'gateway' to the broader world wide Internet. Key industry areas of agency operations, such as Health, Justice, and Education have implemented dedicated communications networks of their own that are connected to StateNet.

The following diagram illustrates the IT Infrastructure environment.

Overview of Environment



Governing Requirements for IT

Government IT infrastructure arrangements underwent a major change in 1993-94. At that time, the then Government initiated a large scale outsourcing contract with the private sector that resulted in a nine year contract with EDS (Australia) Pty Ltd (EDS) for the provision of government IT infrastructure. This contract, that was signed in late 1995, resulted in the outsourcing of practically all Government agency IT infrastructure and implemented a process of consolidation, rationalisation and standardisation for all Government IT infrastructure.

Government mandated security standards for outsourced systems and infrastructure were developed in 1994 concurrent with the EDS infrastructure contract. Key government-wide financial systems for accounts payable, accounts receivable, and human resource management, were also mandated in 1994.

The then Office of Information Technology and its successors, the Department of Information Industries and the Department of Information Technology Services were responsible for leadership, IT strategy, policy, direction, and for implementation and management of the EDS and other major IT outsourcing contracts.

It is relevant to note that these agencies were single focus points with specific responsibilities for the management of certain aspects of Information Technology. Key responsibility for approval of major IT initiatives of Government was given to an IT Cabinet Sub Committee.

During the period of its incumbency, the former Government moved away from the administrative model of a separate agency dedicated to Information Technology matters, and this role was transferred to DAIS. In essence, DAIS has, amongst its many other activities, primary responsibility for public sector wide IT strategy, planning, policy, government-wide initiatives, and, direction/guidance to agencies in matters pertaining to IT.

Treasurer's Instructions, the Financial Management Framework, and principles of sound management, require agencies to develop IT Strategic Plans to support their key business operations. Those plans need to be in general alignment with individual agency corporate plans, and the whole-of-government ICT Directions strategy. Agency plans also need to recognise existing government arrangements for IT Infrastructure provision and use of government mandated systems. Furthermore, these plans must conform to the standard architecture requirements for government computer infrastructure.

Other key IT related requirements which must be met by agencies are contained, inter alia, in the Financial Management Framework, Treasurer's Instructions, other directives issued by the Department of Treasury and Finance, and guidance from the Prudential Management Group.

Treasurer's Instructions provide direction on approval processes for IT projects depending on whole-of-life costings and other criteria. Cabinet approval is required in certain matters.

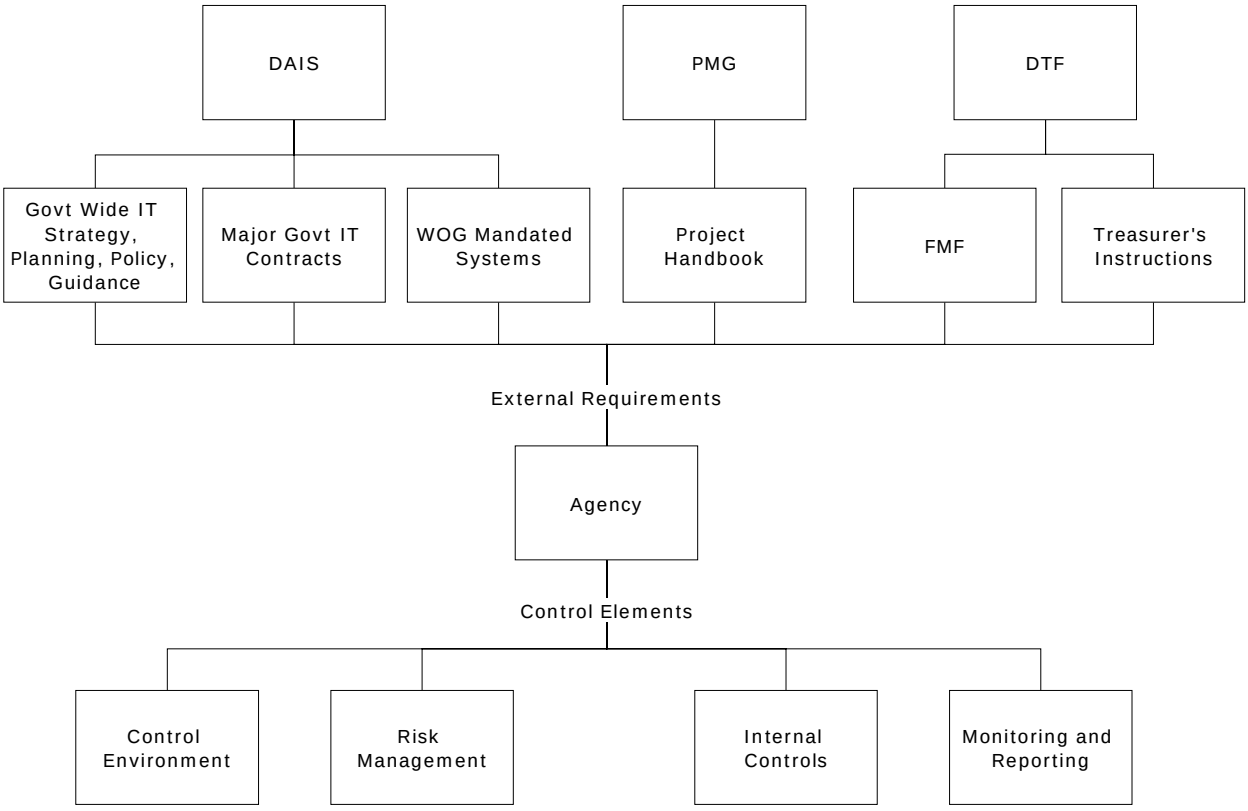
In regard to security control matters, in the period under review ie 2002 and 2003, agencies were mandated to comply with the Government's 'Information Technology Security Standards - In an Outsourced Environment'. This standard outlines both an approach to security development (the Security Development Framework), as well as control measures to combat the security threats of concern to agencies.

In April 2003, the SA Government Information Security Management Framework (ISMF) was approved as the current Information Technology security standards and guidelines for implementation by agencies. That framework is in the process of being fully implemented as part of an overall security program.

The establishment and maintenance of a sound internal control environment, with specific internal controls covering agency systems and processes, is an important management responsibility. That responsibility is emphasised in the Financial Management Framework issued by the Department of Treasury and Finance. Agency responsibility clearly extends to IT matters.

The relevant requirements and control elements are depicted in the chart hereunder.

IT Requirements and Agency Control Elements



AUDIT REVIEW

Fundamental Governance Aspects Examined

The Audit reviews took into consideration matters of a management control nature, that in the opinion of Audit, would ordinarily be regarded as important elements of an overall IT governance framework.

The important elements are described below under key responsibility areas of government.

Executive Government (Cabinet)

- Endorsement of an IT vision, and a whole-of-government IT Plan.
- Endorsement of a framework of IT strategy, policies and standards.

- Consideration by Cabinet of major projects submitted by agencies.
- Ongoing overview of major project status.

DAIS (as Lead Agency for IT in conjunction with other Agencies)

- Development of IT vision and whole-of-government IT plan, with associated strategy, policy and standards framework.
- Implementation and management of whole-of-government IT projects.
- Management of major government IT contracts with the private sector.
- Provision of direction/guidance to agencies in respect of IT matters.
- High level monitoring and reporting to Executive Government the status of major whole-of-government and agency IT projects.

Agencies

- Maintenance of an agency IT strategic plan.
- Establishment of an internal control framework in accordance with the Treasurer's Instructions, Financial Management Framework, and government IT security control requirements.
- Submission of major IT projects to Cabinet for approval in terms of Treasurer's Instructions.
- Implementation of key project governance and risk management arrangements. This would include a steering committee structure/role, business case, specification of system requirements, contract and legal issues, recording and monitoring, system acceptance and post-implementation review.
- Regular reporting to the Chief Executive and Cabinet of major IT project status.
- Provisions for continuity of business operations.

The review of governmental processes including the role of DAIS and agency management and control, has provided Audit with a sound basis for assessment of the leadership and direction provided by DAIS and Executive Government, and of the management, security and control exercised by individual agencies over major IT developments and operations. Audit's key observations are as stated hereunder.

SOME KEY AUDIT OBSERVATIONS

As mentioned previously, past and more recent reviews undertaken by Audit have identified inadequacies in IT management and control. This has included inadequacies regarding control, project, and risk management arrangements.

Consolidated Government IT Plan and Policy and Standards Framework

Audit acknowledges some significant work undertaken by DAIS in the release in August 2003 of the 'vision' planning guidance document titled 'ICT Directions' that is referred to above. That 'vision' document, however, has no specific focus on outcomes or mechanisms that would clearly identify planned and approved major IT projects, facilitate prioritisation of those projects and enable effective monitoring of significant developments already approved by Cabinet. It does not, in my opinion, contain, in a

comprehensive form, the type of information expected in a government ICT Plan. By way of example, a government ICT plan would be expected to, inter alia, include the following matters:

- An analysis of business and ICT future operational requirements and issues.
- Identification of specific opportunities and Cabinet approved projects.
- Prioritisation of those opportunities and projects.
- Allocation of funding and other resourcing to undertake those priority initiatives.
- Management and tracking of performance as to those initiatives relative to Cabinet approval, funding and timeframes.

DAIS has acknowledged that further development of policy and standards is required.

Monitoring and Reporting to Cabinet of Major IT Projects

Under current administrative arrangements the monitoring of major IT project developments, as approved by Cabinet, in my opinion, is inadequate. This includes the matter of lack of timely status reporting to Cabinet, both at a whole-of-government and agency level.

There is no clear responsibility and accountability for monitoring of government major Cabinet approved IT project developments and no effective existing mechanisms to enable it to be undertaken. Furthermore, arrangements for the advice to, and the consideration by, Cabinet in a timely manner of potential problems is inhibited.

The regular monitoring of Government planned IT developments is essential. Without timely and relevant information, Executive Government is not in a position to fully harmonise like activities across agencies, measure performance, and maximise efficiencies. The implementation of a whole-of-government IT plan, against which the status of major agency IT projects can be regularly monitored would facilitate such consolidated reporting to government.

Agencies Planning and Management for IT, Project Development and Risk Management Practices

In my opinion, for reasons discussed in other Parts of this Report, a number of agencies have paid inadequate attention to strategic planning and management for IT and have not maintained effective risk management practices. The areas requiring attention include, formal IT strategic plans aligned with agency business plans, arrangements for continuity of business operations, security control provisions, and adequate formal agreements with the private sector for IT service provision.

Risk management is a holistic process designed to aid management by providing proactive steps to identify, classify and prioritise risks, and then implement mitigating strategies. Many agencies have not proactively addressed the risks to continuity of agency systems or services since consideration was given to the Year 2000 millennium bug problem. Even where those agencies have taken steps to plan to cater for a disruption in systems or services, those plans have rarely been tested. Another example of inadequate risk management practice is in the arrangements made when contracting with the private sector.

It is important that agencies adopt appropriate IT strategic planning project and risk management practices. These arrangements should be regularly revisited, particularly in

areas such as purchasing of IT services, operations management, the protection of information assets, and business recovery arrangements.

Government Initiated Reports

With reference to the important need for improvement in whole-of-government and agency governance and management of ICT operations, it is of interest to note that in the May 2002 Report, 'Public Sector Responsiveness in the 21st Century'[4] the following observations were made:

> *… evidence has been provided to the Task Force which shows that some major strategic planning activities have been limited in their effectiveness as a result of:*
>
> - *insufficient coordination between the whole-of-government vision and priorities, and departmental plans and budget bids;*
> - *a tendency to finalise whole-of-government strategies after the budget has been allocated;*
> - *unclear articulation of priorities and desired outcomes …*
>
> *The Task Force believes collaborative development of vision and strategic priorities helps to create shared ownership, assists in the identification of 'champions' for particular outcomes and provides a clear articulation of the interdependencies between government departments …*
>
> *… Key indicators and targets should also be built into whole-of-government strategies to allow progress to be measured openly and transparently. It is also important to regularly review outcomes, plans and programs, and to take remedial action where necessary …*

It is also of interest that a Report, in January 2003, on 'Standard Corporate ICT Infrastructure Strategy'[5] produced for the Victorian Government, recommended, amongst other matters, that a '… CIO Office should be established at a whole-of-government level'. The Report further went on to comment:

> *There are three broad sets of ICT processes relating to the whole-of-government CIO office functions:*
>
> - *ICT strategy and planning.*
> - *Architecture, policies and standards development.*
> - *Management of ICT investments. …*
>
> *… Three factors appear to be crucial to the success of a CIO office: (i) it must provide ICT leadership and advocacy across government; (ii) it must be a partner to departments; and (iii) it must have sufficient authority and resources to make a difference to the management of ICT across government and to the role of ICT in enabling government service delivery. …*

---

4 Public Sector Responsiveness in the 21st Century – A Review of South Australian Processes, May 2002.

5 State Government Victoria, Standard Corporate ICT Infrastructure Strategy, Final Report, 31 January 2003, The Boston Consulting Group.

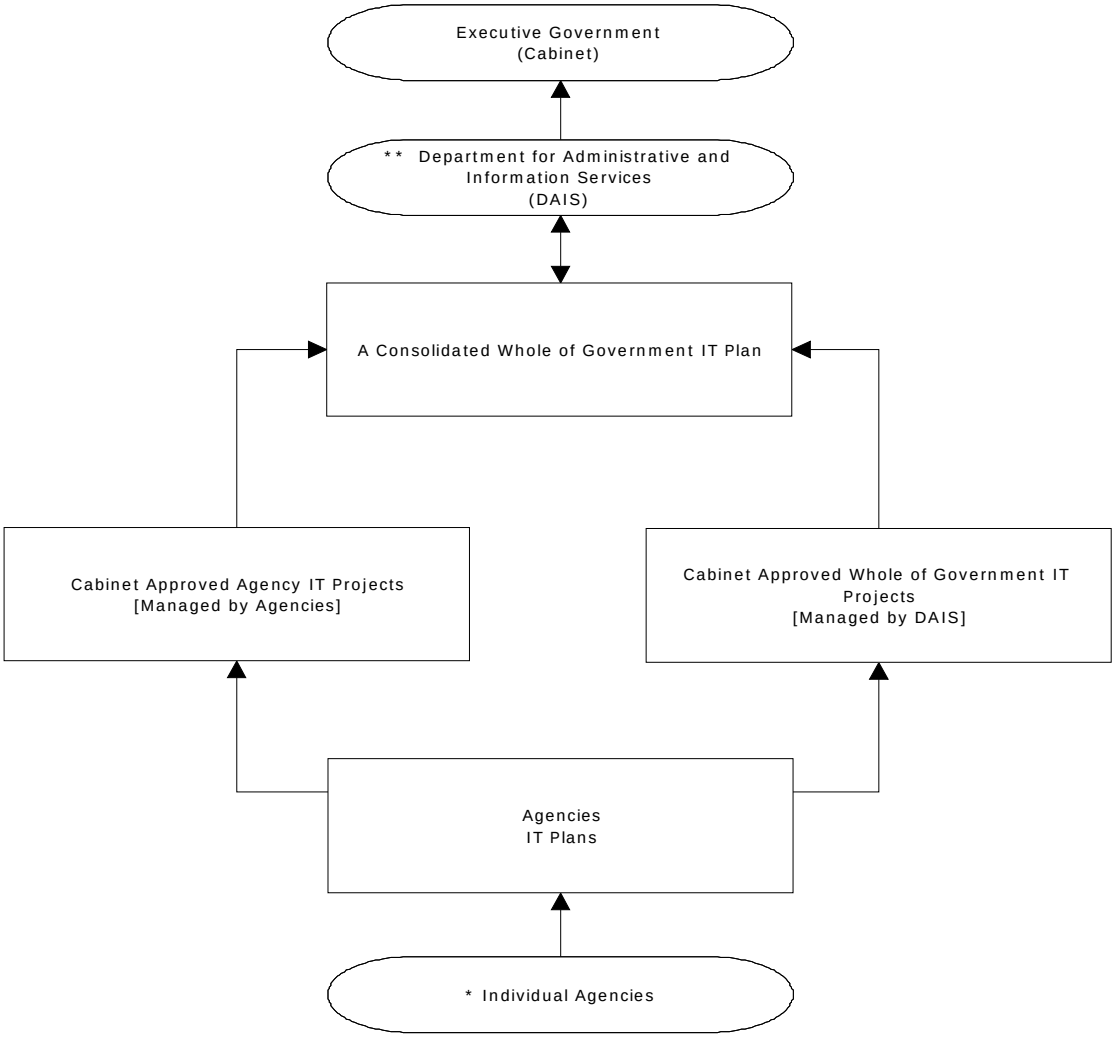
… A program office function is necessary to ensure accountability and drive successful implementation of large ICT projects, and the CIO office is uniquely placed to consolidate the high-level tracking and monitoring of projects, independent of any one department. …

… [individual agencies] should report their progress in implementation and realisation of benefits to the program office maintained by the CIO office, …

AUDIT VIEWPOINT

Fundamental Governance Arrangements for Monitoring and Reporting

Audit considers that fundamentals of monitoring and reporting on the Cabinet approved IT developments of government and agencies, would operate as follows.



* Individual Agencies
Prepare and monitor their IT Plans; Provide information to DAIS to facilitate DAIS maintained consolidated Whole of Government IT plan; Submit specific reports to Cabinet on the progress of Cabinet approved IT projects.

** DAIS (as lead IT Agency).
Prepare and monitor a consolidated Whole of Government IT plan; Report to Cabinet on the progress and status of Cabinet approved IT projects as against the consolidated Whole of Government IT plan expectations.

As mentioned previously, the current process has limited effectiveness in that there is no whole-of-government IT plan of major IT projects of government and its agencies against which monitoring and reporting to Executive Government can occur. Audit's reviews have also found that agency reporting on the status of implementation of major projects back to Cabinet, particularly where problems have arisen, is inadequate. There is a pressing need for improvement in these processes.

Considering the findings and recommendations from Audit's reviews and their consistent messages, the present inadequacies tend to indicate a need for a centrally managed function with a whole-of-government perspective.

An effectively coordinated approach would facilitate the communication of a consistent message to agencies regarding matters of fundamental importance concerning IT management and operations. These matters would include the ability to more effectively monitor aspects of Information Technology (with some emphasis on projects under development, information security management, and strategic management generally). Such an arrangement would also allow for the provision of assistance/advice where it is deemed necessary. This would complement the work of other governance related bodies such as the Prudential Management Group.

Some Relevant Observations of the Public Sector Review Report of May 2002

It is relevant to note that the Task Force Report, of May 2002, on 'Public Sector Responsiveness in the 21st Century', included the following observations:

> *… Governance is the link between the activities of management and staff, and the government's vision … It is the means by which Cabinet's vision for the State is conveyed to public sector management, and by which management's actions are reported back to Cabinet and measured against Cabinet's expectations.*[6] *…*
>
> *… The Task Force was informed there is currently no mechanism for monitoring the implementation of Cabinet decisions. The Task Force believes the inclusion of a concise implementation plan in each Cabinet submission would help to ensure that both the Government and relevant agencies have a common understanding of what is expected in the proposal's implementation.*
>
> *Monitoring of the key milestones outlined in this plan for review and feedback would also help to ensure that Cabinet is advised of progress if and when appropriate. …*

The Report goes on to say:

> *… Comment was also made that an overall framework, which brought together the different elements in a meaningful way, had not been clearly defined and articulated. Among other things, this made it more difficult to make sense of the myriad of projects, initiatives, policies, processes and other requirements, …*

---

6 Owens, L W (unpublished), 'Public Governance and the Government Management Framework. A Proposed Model to Support GMF Implementation'. Paper to the Senior Management Council, 1999.

… The Task Force recommends that the Department of the Premier and Cabinet develop a whole-of-government strategic planning framework and process, which ensures that:

- *the Government's vision, priorities, outcomes and performance measures are clearly defined …*

There are of course, a number of ways in which government could address the matters raised by Audit. The mandate and responsibility for such clearly rests with the Executive Government. The following suggestions put forward by Audit reflect one approach to addressing these matters.

SUGGESTIONS FOR IMPROVEMENT

The following suggestions were formally forwarded to DAIS in two management letters ie in August and October 2003.

Audit recognises the differing role responsibilities of Executive Government, through the MPICC, DAIS as the lead agency for ICT and individual agencies. Audit's suggestions included in the management letters were provided against that background.

Executive Government

To enable adequate coordination and control, in my opinion, there should be a clearly stated Government IT Plan. That plan should identify each major IT project development, either initiated by DAIS in a whole-of-government context, or agency initiated, and as approved by Cabinet. The plan would also include a statement of the key performance indicators, including costs, implementation timeframes, and service delivery outcomes.

The status of those Cabinet approved major IT project developments should be regularly monitored and reported to Executive Government against the approved Government IT Plan timeframes and outcomes. This reporting would include both whole-of-government projects and individual agency projects.

DAIS

To facilitate adequate coordination and a control of IT operations, in my opinion, the role/responsibilities of DAIS should be enhanced, notwithstanding the existing and continuing responsibilities of individual agencies. The enhanced role would include responsibility for the development of a Government IT Plan and monitoring and reporting as outlined herein. Formulation and 'ongoing maintenance' of a Government IT Plan and the reporting to Cabinet as to compliance with and/or variations to that Plan would be a DAIS responsibility.

An arrangement such as this would give a 'single point of focus' and 'accountability' for the monitoring and reporting to Cabinet. Audit considers that role could be undertaken by DAIS in the context of a whole-of-government Chief Information Officer position as suggested by Audit in the management letter communications that have already been made. The exact nature of this arrangement would require some consideration by DAIS.

Reporting should address not only progress against Government IT Plan expectations, but should also identify, in a timely manner, projects which have encountered problems. These matters can be brought to the attention of Cabinet.

In my opinion, DAIS is ideally placed to undertake this monitoring and reporting role. DAIS currently has a major role in the initiation and development of ICT Directions strategy, IT Policy, and IT Standards. It is also responsible for the implementation and management of major whole-of-government IT projects.

Agencies

With respect to IT initiatives that are proposed for implementation at the individual agency level, in my opinion, prior to the submission of proposals for Cabinet approval, the following matters must be adequately addressed:

- Agency business plans and approved IT strategic plans.
- Implementation Plan for the project, including periodic update status provision to Cabinet.
- Evidence of appropriate project and risk management governance.

Individual agency Chief Information Officers would, as a matter of course, report progress and status of all major approved agency IT initiatives to the agency Chief Executive and to Cabinet. Reporting would be in accordance with implementation plan requirements as advised in initial Cabinet submissions. Agencies would also have responsibility to report to DAIS to enable facilitation of DAIS's responsibility of consolidated reporting to the MPICC against a Government IT Plan.

The matters pertaining to individual agencies would require the development of a formal documented accountability/responsibility framework for compliance requirements in respect of the roles and responsibilities of agencies and DAIS.

Audit recognises that implementation of the approach and accountability/responsibility framework would require consideration of the appropriateness and applicability of existing requirements documented in current directives, including the Treasurer's Instructions, Financial Management Framework, Prudential Management Group Framework, and Cabinet approval processes.

Prudential Management Group

It was also considered that the Prudential Management Group, or similar, would undertake regular audits of the project and risk management arrangements for all major approved IT initiatives of government agencies. This would provide an independent 'health check' on a timely basis to ensure potential or existing problems are readily brought to attention and addressed.

DAIS CONSIDERATION AND RESPONSE TO AUDIT SUGGESTIONS

DAIS formally responded in a comprehensive manner to the two management letters forwarded by Audit and the matters raised have been the subject of discussion with the Department.

In its responses, DAIS outlined a number of initiatives taken during 2002 and 2003 to strengthen ICT governance arrangements. Those initiatives are acknowledged and have been outlined under the heading 'Recent Government Developments' in this Part of this Report.

DAIS also recognised that further improvement was required in a number of areas of ICT governance at a whole-of-government and agency level and advised of some matters presently under consideration that would significantly address those matters.

Specifically, DAIS recognised Audit's concerns in relation to the monitoring and consolidated reporting of the status of ICT matters in the South Australian public sector. As many of the matters to be addressed are at a whole-of-government, as well as agency level, DAIS indicated that this would require considerable engagement with agencies and other key stakeholders in developing and agreeing a formal program of work in respect to the approach.

The initiatives being considered by DAIS will be based upon a consolidated approach for government. DAIS would play a facilitating role in these arrangements, helping deliver the outcomes expected from a whole-of-SA Government Chief Information Officer as suggested by Audit.

DAIS recognised that the governance and management of ICT across the SA Government must accommodate the complexity of the public sector environment. Leadership in ICT matters, and effective governance of ICT is seen as an important requirement for the South Australian Government, and accepted as a major responsibility by DAIS.

The initiatives under consideration by DAIS have identified the need for a framework that addresses six key areas of ICT governance and management, ie:

- leadership in ICT
- ICT planning
- investment and prioritisation
- ICT policy
- monitoring and control
- coordination and compliance.

Some key elements and requirements that are inherent in the initiatives being considered are:

- identification and review of the major business systems and applications currently in use within the SA Government;

- identification of major projects 'currently under way' or 'proposed' at a departmental and whole-of-government level;

- establishment of a register of Cabinet approved ICT-based projects;

- establishment of formal reporting arrangements for Cabinet approved ICT projects;

- development of requirements for independent project assurance of major ICT projects.

- further expansion of the role of the Major Projects and Infrastructure Cabinet Committee to consider aspects of ICT investment, project and risk management and to oversight major ICT projects on behalf of Cabinet;

- enhancement of the 'ICT Policy, Strategy and Standards Steering Committee' role to support the MPICC;

- development of an ICT strategic investment plan, based upon ICT Directions. This to be undertaken in association with the 'SA Government strategic plan' currently under development by the Department of the Premier and Cabinet;

- development and endorsement of a fundamental set of principles addressing the common deployment and management of ICT and ICT based services across the SA public sector;

- further documenting the responsibilities and accountabilities for ICT planning and management at a whole-of-government and departmental level;

- development in collaboration with agencies of a recommended approach to improve and achieve greater commonality in agency and departmental ICT planning;

- the requirement for agencies to develop an ICT strategic plan consistent with their policy and service objectives and establish their investment plan (plan for action);

- progressive revision of ICT policy and standards in association with the Future ICT Services Arrangements initiative.[7]

- progressive review of the government's arrangements for ICT service provision, monitoring and management;

- redrafting of requirements for major project submissions to include explicit consideration of potential cross-departmental synergies and business opportunities and common (shared) infrastructure requirements and standards;

ACTION TOWARDS RESOLUTION

As mentioned above, DAIS has under consideration a series of initiatives to address identified weaknesses in IT Governance and Management at whole-of-government and agency levels.

These initiatives will be developed in conjunction with other agencies. They will address key aspects of Audit's concerns in monitoring and reporting to Executive Government of the ongoing status of major IT project developments. It is not however, clear as to whether the approach would include measurement and reporting of their status against any consolidated IT plan view of Executive Government and/or agency expectations.

Due to the fact that these initiatives are currently under consideration and have not been formally adopted, DAIS's response, understandably, was not specific in details as to its

---

[7] See above under 'Recent Government Developments'.

operation in practice. Notwithstanding, implementation of these initiatives along the lines advised would significantly address the matters raised by Audit.

Considerable engagement with agencies and other key stakeholders will be required in developing and agreeing a more formal program of work. DAIS advised that this collaboration and the resultant proposed initiatives would require that a submission be made to Cabinet by the Minister for Administrative Services. DAIS anticipated that consultation and development of this Cabinet submission would be undertaken during late 2003 and early 2004 in accordance with any directions that may be given by the Minister.

CONCLUDING COMMENT

As a matter of good public administrative practice, it is to be expected that the Government should be in a position to clearly articulate, at a whole-of-government level, the current position/status of all major planned and approved IT developments of government and its agencies, as measured against a consolidated whole-of–government IT plan. That is not presently the case due to the absence of such a consolidated plan. This is not to say that government is unaware of the status of certain major developments, or that indeed there is no monitoring of certain individual agency IT projects by the lead agencies.

In my opinion, implementation of a whole-of-government IT Plan that clearly identifies, coordinates, and controls major approved IT projects, would facilitate the prioritisation and effective monitoring of those projects. This would enable the Executive Government (Cabinet) to receive timely reports and to be in a position to be able to exercise appropriate oversight and control. Under the existing arrangements this oversight and control does not always occur with the consequence that, some projects have not, in Audit's opinion, been adequately managed and have resulted in adverse financial outcomes for government.

Clear responsibility and accountability as to outcomes in information technology service provision and developments at a whole-of-government and agency level is necessary. Proper administrative arrangements will enable the Government to have an adequate level of assurance regarding the ability of public sector agencies to deliver in accordance with realistically agreed expectations, now, and into the future.

The matters discussed in this Chapter are of fundamental importance having regard to the extent to which IT underpins the operations of government in this State. In the following Chapters several specific issues associated with IT management and operations are discussed.

PART 2 — PROJECT AND RISK MANAGEMENT FOR MAJOR IT DEVELOPMENTS

PART 2 — PROJECT AND RISK MANAGEMENT FOR MAJOR IT DEVELOPMENTS

TABLE OF CONTENTS

PART 2 — PROJECT AND RISK MANAGEMENT FOR MAJOR IT DEVELOPMENTS

TABLE OF CONTENTS

CHAPTER 2 — REVIEW BACKGROUND AND KEY AUDIT FINDINGS AND COMMENTS

BACKGROUND

Introduction

This Part of this Report provides an insight into common problems that have been encountered in agency management of some large IT project developments that have been reviewed by Audit. There are a number of well documented cases both within Australia and internationally of large-scale IT projects experiencing major developmental and/or implementation problems or, in some cases, failing completely.

It is principally the identification and regular monitoring of these major IT project developments and the need for reporting back to Cabinet that has been the subject of comment in the previous Chapter. The importance for this is demonstrated by the significant problems that can emerge when such projects do not run to plan and are not subject to tight agency management control, including timely monitoring at the highest level of government.

Audit Mandate

The Audit review process was conducted pursuant to section 36 of the *Public Finance and Audit Act 1987.*

Governing Requirements for IT

Principally, key IT related requirements which must be met by agencies are, inter alia, contained in the Financial Management Framework and Treasurer's Instructions and other directives issued by the Department of Treasury and Finance and guidance from the Prudential Management Group.

The Financial Management Framework outlines the requirement for agency management to implement and document policies and procedures that result in effective control over all significant operations of the agency. The development and implementation of major IT systems and facilities are significant in the operations of most public sector agencies.

As noted in Part 1 of this Report, Treasurer's Instructions provide direction on approval processes for IT projects depending on whole-of-life costings and other criteria. In particular, Treasurer's Instruction 17 has been promulgated to require public sector initiatives to be evaluated in line with guidelines issued by the Department of Treasury and Finance and to require them to be consistent with the objectives of the South Australian Government. It also specifies the approvals required before proceeding to implement public sector initiatives based upon a series of monetary thresholds.

One key requirement is that each Chief Executive shall ensure that proposed initiatives are clearly linked to, and are consistent with, strategic plans of the agency, and that those plans underpin the agency's corporate objectives as directed by the Government.

When entering into a public sector initiative, the following approvals to proceed need to be obtained at the completion of the concept evaluation phase:

- The Chief Executive or other authorised officer, where the estimated cost of the initiative does not exceed the amount of the standing authority delegated in accordance with this instruction, or $500 000, whichever is the lesser.

- The Minister, where the estimated cost of that initiative exceeds the above authority, but is less than $4 million.

- Cabinet, where the estimated cost of that initiative is equal to or greater than $4 million.

With regard to security control matters, in the period under review, agencies were mandated to comply with the Government's 'Information Technology Security Standards - In an Outsourced Environment' promulgated by the then Office of Information Technology in December 1994. This document outlines both an approach to security development, as well as control measures to combat the security threats of concern to agencies.

In April 2003 a new SA Government Information Security Management Framework (ISMF) was approved as the current Information Technology security standards and guidelines for implementation by agencies. That framework is in the process of being fully implemented as part of an overall security program.

AUDIT REVIEW

Review Coverage

From a whole-of-government perspective, this Part of this Report looks at the electronic commerce procurement project managed by DAIS. This was to have delivered efficiencies and savings under the Government's 1998 procurement reform strategy.

Comment is also provided on the whole-of-government human resource management system (CHRIS) and the DECS Human Resource Management System replacement.

The sensitive area of medical information has been addressed with review of the Oacis programme of the Department of Human Services. Oacis will be fully implemented in 2005.

Other agencies and projects selected cover electronic commerce facilities and web sites for financial transaction processing of motor vehicles and drivers licenses, and the electronic lodgement of court claims. The revenue raising area of taxation is addressed with a review of the Department of Treasury and Finance, 'RevNet' project.

In addition, Audit has reviewed a new system development for the Water, Land and Biodiversity Conservation agency.

Fundamental Aspects Examined

The reviews included in this Part of this Report have paid particular attention to key aspects of Executive Government and agency IT governance. This has included matters concerning the management of the risks and control requirements, with respect to IT projects.

The respective responsibilities can be stated as follows:

Executive Government (Cabinet)

- Consideration by Cabinet of major projects submitted by agencies.
- Ongoing overview of major project status.

DAIS (as Lead Agency for IT in conjunction with other Agencies)

- Implementation and management of whole-of-government IT projects.
- Management of major government IT contracts with the private sector.
- Provision of direction/guidance to agencies in respect of IT matters.

Agencies

- Development of IT strategic plans.
- Establishment of adequate agency internal controls in accordance with the Financial Management Framework promulgation and as required by mandated Government IT security controls.
- Obtaining Cabinet approval for major IT projects in terms of Treasurer's Instructions.
- Implementation of key project governance and risk management arrangements, including steering committee structure/role, business case support, system requirements, contract and legal issues, recording and monitoring, system acceptance and post-implementation review.
- Regular reporting to the Chief Executive and Cabinet of major IT project status.
- Provision for continuity of business operations.

KEY OBSERVATIONS AND FINDINGS

Governance Arrangements

At an Executive Government level, Audit found that certain high level governance arrangements were not clearly defined and coordinated. These matters are the subject of comment in Part 1 of this Report.

One particular matter relates to the absence of a consolidated whole-of-government IT Plan that would facilitate ongoing Executive Government prioritisation of major IT initiatives and overview of progress status of major project developments in terms of Cabinet approved arrangements.

Specific IT Project Review Issues

In respect of specific IT projects that have been reviewed by Audit over the past two years, Audit has identified some common issues arising from those reviews. A summary of these issues is as follows:

- Little progress in the introduction and take up of government-wide electronic procurement processes in South Australia and achievement of planned savings under the procurement reform program.
- Project delays and extended timeframes for completion.
- Lack of advice to Cabinet or the Prudential Management Group of significant change in status of projects or periodic status reports.

- Inadequate recording/monitoring of project costs and benefits.
- Inadequacies in agencies' risk and project management arrangements when outsourcing with the private sector.
- Risk management arrangements not reviewed and updated on a regular basis.
- Operation of the Bizgate e-commerce facility without formal agreements in place with government agencies or the private sector IT service provider.

Interstate Experience

In a recent article[8] on IT projects, a specialist project manager from a leading international Audit organisation, noted that there was a long history of failures with ambitious technology projects of all sizes. The article also discussed problems experienced with respect to recent IT project developments within Australia emphasising the truth of the well worn phrase that 'history repeats itself' for those who do not heed its lessons.

As an illustrative example of the problems being experienced, a recent review of Sydney Water's Customer Information and Billing System (CIBS), by the New South Wales Auditor-General,[9] found amongst other matters that:

- the project was approved without a corporate information technology strategy;
- management did not always report important issues to Sydney Water's Board of Directors in a clear, complete and timely manner;
- the Board did not oversee the project as effectively as it might have. Its understanding of the project, in light of its complexity, was limited;
- risk management was not effective at the corporate and project levels;
- the culture of Sydney Water suggests a belief that the outsourcing of major projects will effectively transfer all risks to the contractor;
- Sydney Water did not adequately disclose the status of CIBS in its 2002 Annual Report.

INDIVIDUAL AGENCY REVIEWS

Specific agencies and IT Project developments reviewed and commented on in the following Chapters of this Part of this Report are:

Department for Administrative and Information Services	Bizgate E-Commerce for Procurement
Courts Administration Authority	Electronic Lodgement Project

---

8 Australian Financial Review, Tuesday, 7 October 2003, p 29 'Government problems revealed'.

9 NSW Auditor-General's Report to Parliament 2003, Volume One – Review of Sydney Water's Customer Information and Billing System.

Department of Education and Children's Services	Human Resource Management System (HRMS) Replacement
Department of Human Services	Complete Human Resource Information System (CHRIS)
	Open Architecture Clinical Information System (Oacis) Project
Department of Transport and Urban Planning — Transport SA	Registration and Licensing Initiative
Department of Treasury and Finance — RevenueSA	RevNet Project
Department of Water, Land and Biodiversity Conservation	Water Information and Licensing Management Administration System

The reviews presented examine IT project developments and the measures taken to mitigate risks, including those previously identified by Audit. The focus of the case studies is on matters of a project and risk management nature.

My Report for the year ending 30 June 2001 also considered a particular case study on the operations of 'Bizgate'. Bizgate is a key e-commerce initiative of the South Australian Government that was then managed through the former Department of Industry and Trade. As foreshadowed in that Report, that case study is briefly revisited herein.

CONCLUDING COMMENT

Arising from the review of several IT projects that have been undertaken over recent years, it can be said that inadequacy of the control environment has resulted in substantially incurred costs and delay some of which was avoidable. The frustration of the hope for the achievement of administrative efficiencies is obvious.

This is illustrated in the whole-of-government projects reviewed, notably the DAIS e-commerce for procurement initiative, and the Human Resource Management Systems being progressed in the Health and Education sectors.

Whilst matters arising from the reviews of the specific IT projects have been formally communicated to the responsible individual agencies, I have also formally communicated to DAIS, as the lead agency for information technology, the major common themes. Responses to those formal communications have been received from the individual agencies and DAIS.

Overall IT Governance and Management

The formal Audit communication to DAIS suggested the introduction of a consolidated whole-of-government IT Plan and the establishment of a whole-of-government Chief Information Officer position. That Officer would report on the ongoing status of major Cabinet approved IT project developments, and of overall progress against the consolidated IT Plan. This report would be made to the Chief Executive DAIS, and the Major Projects and Infrastructure Cabinet Committee. In this way Executive Government would be in a position to receive timely reports of progress of major IT

developments and exercise appropriate oversight and control and implement corrective action where appropriate.

It was also suggested that the Prudential Management Group, or similar, would undertake regular audits of the project and risk management arrangements for all major approved IT initiatives of government agencies.

Agency Specific Arrangements

With respect to individual agencies, where problems have been encountered they stem broadly from inadequacies in planning, project monitoring and reporting and risk management arrangements.

The formal Audit communication to DAIS suggested that these areas could be improved by agencies ensuring that the following antecedents, are in place prior to submitting IT project proposals to Cabinet for approval. Notably, the development of:

- agency business plans and approved IT strategic plans;
- implementation plan for the project, including periodic update status provision to Cabinet;
- evidence of appropriate project and risk management governance skills and processes.

To assist with monitoring and reporting, individual agency Chief Information Officers would report progress and status of all major approved agency IT initiatives to the agency Chief Executive and to Cabinet. Reporting would be in accordance with implementation plan requirements as advised in initial Cabinet submissions.

CHAPTER 3 — AGENCY REVIEW: DEPARTMENT FOR ADMINISTRATIVE AND INFORMATION SERVICES

BIZGATE

Background

Bizgate is a significant e-commerce initiative of the South Australian Government. Bizgate provides a diverse range of e-commerce services to over 30 government and local government organisations including the provision of online forms and payment services.[10]

Audit's initial review of Bizgate was the subject of specific comment in my 2001 Report. At that time Audit highlighted certain areas requiring attention. Bizgate was under the administrative responsibility of the then Department of Industry and Trade. The matters raised at that time related to policy, management reporting and control arrangements, ongoing liaison with DAIS, contract and service level agreements, continuity of operations, system changes, and intellectual property rights.

Further, there were a number of client agencies without formal agreements with Bizgate. There was limited detail available on matters such as service levels, continuity of operations, intellectual property rights, and required security controls in those agreements that had been documented.

An area of concern to Audit has been the lack of appropriate management reporting and the control arrangements within the agency responsible for Bizgate.

Update Review Status

During 2003 Audit followed up matters with respect to Bizgate developments. More recently, in September 2003 Audit undertook a follow up review and sought a formal update status from DAIS regarding a number of matters, including the transfer of Bizgate operations to DAIS.

DAIS Response *— In October 2003 DAIS advised that:*

- *Bizgate was transferred to the Government ICS area of DAIS as of 1 July 2003;*
- *a due diligence process was undertaken to identify issues, risks, requirements and possible business modelling;*
- *negotiations are taking place with the external service provider in relation to formulation of a service level agreement and contract;*
- *intellectual property issues associated with Bizgate are being addressed;*
- *work has begun on the development of a business model (cost recovery) in conjunction with Bizgate customers for implementation in 2004-2005.*

Characteristics of Project

In summary, this project has demonstrated the following characteristics:

- Informal policy, management reporting, and control arrangements.
- Delay in finalisation of revised management arrangements.
- Client agencies without formal service level agreements with Bizgate.

---

[10] www.bizgate.sa.gov.au

ELECTRONIC COMMERCE FOR PROCUREMENT INITIATIVE

Background

In May 1998, the South Australian Government launched its Procurement Reform Strategy. The aim of this initiative was to improve government purchasing and achieve better value for money via electronic commerce (e-commerce). An integral part of the Procurement Reform Strategy was the Electronic Commerce (for Procurement) project, which included the development, and eventual whole-of-government implementation, of an Integrated Electronic Purchasing Solution (IEPS) by December 2000.

It was envisaged that the Procurement Reform Strategy would generate $72 million in ongoing annual savings, of which $28 million were expected to flow from Electronic Commerce (for Procurement) activities (with $18 million being attributable to the IEPS). These savings were expected to be achieved through a reduction in transaction costs due to streamlining of administrative processes, and through better buying practices enabled by improved information management.

Once developed, the IEPS would be progressively implemented throughout government with time frames to be determined on an individual agency basis.

The then Cabinet agreed that DAIS would lead the Electronic Commerce (for Procurement) initiatives, including the development of the IEPS, working collaboratively with other key local and interstate government agencies. To facilitate and manage this task, an Electronic Commerce Steering Committee was formed, reporting directly to the Deputy Chief Executive, DAIS (the Chair of State Supply Board). Strategic guidance was provided by the Government Purchasing Task Force (GPTF). The GPTF reported directly to Cabinet.

In December 1997, Cabinet approved the development of electronic systems (stage one) at $750 000.

A tender process for the IEPS began in November 1998, and the final recommendation of a solution provider was approved by the State Supply Board in September 1999, and Cabinet advised of the tender outcome. The selection process culminated with the execution of the contract with the successful respondent in October 1999.

Essentially, Cabinet approved the project in 1998 with the expectation of providing basic access to the IEPS across all agencies by December 2000. Cabinet also gave approval for business cases for Stages 2 and 3 to be submitted for its consideration in early 2000.

Implementation

The IEPS implementation strategy comprised three stages.

- Stage 1 involved the implementation and trial of the IEPS (known as E-Purchase SA) at a small number of DAIS sites, as well as a suburban public hospital.
- Stage 2, the full implementation of E-Purchase SA within DAIS.
- Stage 3, the whole-of-government rollout, was envisaged to occur subsequent to achieving success with the trial stage.

During late 2000 and 2001, unforeseen circumstances with the solution provider required legal negotiations between DAIS and the provider. A Variation Agreement was signed between DAIS and the solution provider to allow for trial implementations of the software in agencies beyond DAIS for Stage 2. The Stage 2 contract with the solution provider was executed in September 2001.

Stage 3 of the agreement was also varied. The original agreement required the Government to move from 700 software licences to 7000 licences in one step. This was modified to allow Departments to adopt the software on an agency-by-agency basis. Agencies are required to fund their own implementations. However, implementation of E-Purchase SA beyond DAIS is currently limited to a few trial sites, with full Stage 3 implementation not envisaged in the near future.

Audit Focus

The review of the E-Purchase SA project addressed matters of project management and achievements, and risk management arrangements. In particular, Audit assessed the adequacy of business plans; project planning, approvals and management; and monitoring and reporting arrangements.

Audit Findings and Recommendations

There has been significant delay in the progression of the project to the envisaged whole-of-government (Stage 3) implementation. Cabinet approved the project with the expectation of providing basic access to the Integrated Electronic Purchasing System software across all agencies by December 2000.

Cabinet has not been kept abreast of the fact of the reasons for the delay in implementation or current status with respect to the project. A revised business case was to have been submitted for Cabinet consideration in early 2000. This has not happened.

DAIS sought funding for the progression of the initiative through the budget negotiation bilateral meetings for the years 2000-01 and 2001-02. These bids were unsuccessful. DAIS, through the 'Across-Government Savings Strategy Steering Committee', initiated a detailed consultancy to deliver a report on 'Procure - To Pay E-Business Systems Integration'.

Governance via a formal Steering Committee was in place for Stage 1 of the project. There was no such Steering Committee in place beyond this stage of the project.

Notwithstanding the delay in the progression of the project, Audit's review identified that project expenditure is still being incurred but recording and monitoring of costs against approved budget allocations has not been maintained throughout the project and accurate costs could not be obtained.

The benefits expected to be realised from the E-Purchase SA initiative of $28 million from the Electronic Commerce (for Procurement) activities are unlikely to be realised. These benefits are dependent upon achieving Stage 3 of the implementation.

Audit considered it a matter of importance that DAIS reconfirm with Cabinet its status as lead sponsor of the initiative and the future direction of the project. More importantly, Audit considered DAIS should include an assessment of this initiative's current functionality, capability and standing in relation to initiatives taken interstate.

The implementation of the planned government-wide electronic commerce for procurement initiative in South Australia has not progressed as quickly as envisaged in this State. The South Australian procurement initiative is of a modest size in comparison with recent developments in New South Wales and Victoria for the contracting out for provision of electronic procurement at a whole-of-government level.

The longer the delay in the implementation of an e-procurement solution or strategy, the higher the risk that individual agencies may develop their own e-procurement solutions, different to an approach that may have a whole-of-government perspective/benefit. This may result in a fragmented system and loss of efficiency.

In consideration of the project's changed circumstances since approval by Cabinet in 1998, Audit submitted certain recommendations to DAIS in March 2003. Those recommendations were:

- Revise and re-evaluate the strategic direction and business case for this initiative. This re-evaluation should include the conduct of a risk assessment with respect to the progression of the E-Purchase SA initiative and comparison to initiatives taken interstate.

- Convey the results of the re-evaluation as a progress status report to Cabinet for consideration and direction.

- Submit regular periodic reports to Cabinet with respect to the project's status.

- Re-establish, dependent upon the future strategic direction of the project, an appropriate Steering Committee to provide continued guidance and monitoring. Audit believes that there are opportunities for improvement with the presentation of ongoing formal project status reports to governance committees.

DAIS Response *— In April 2003 DAIS advised that e-procurement is not yet seen as a priority for government and no central funds have been available for its implementation. DAIS stated that Departments have competing priorities for funds and have not been able to finance the e-procurement initiative from within their own resources.*

DAIS advised that DAIS and DTF are engaging a consultant to benchmark the government's procurement processes as part of a broader assessment of government processes. This exercise will include a comparison of e-procurement initiatives taken interstate. The second phase of this consultancy will involve the development of a business case for the procurement process, along with other government processes. The procurement business case is expected to be completed by late 2003. DAIS acknowledged it is unlikely that funds will be made available for the implementation of e-procurement across government until the results of this consultancy are known.

DAIS advised that it will action Audit's suggestion to submit reports to Cabinet with respect to the project's status.

A steering committee has been established to oversee the consultancy into the specific government processes that are being investigated. Once the results of the consultancy are known it is expected that individual Steering Committees will be established to oversee any specific initiatives that arise from the consultant's recommendations.

Audit conducted a follow up review and in September 2003 sought further clarification of the project status and any outstanding issues.

DAIS advised in September 2003 that a consultant was appointed to develop a Business Case for the procurement process and that this project was due to be completed in late 2003. The expected outcome of the business case development project is that it will either reinforce the need for an e-procurement system across government or that an alternative strategy for the procurement process will need to be developed. In either scenario, appropriate governance arrangements will be instituted.

In addition, Cabinet approval would be sought by the end of December 2003 to implement any appropriate recommendations that may arise from the project.

Characteristics of Project

In summary, this project has demonstrated the following characteristics:

- A reported lack of funding availability and high level support for the project.
- Project delay and extended timeframe for completion.
- No formal steering committee in place for latter stages of the project.
- Variations to contract arrangements through unforeseen circumstances.
- Lack of advice to Cabinet of significant change in status of project or periodic status reports.
- Risk/Project management arrangements not revisited on a regular basis.

CHAPTER 4 — AGENCY REVIEW: COURTS ADMINISTRATION AUTHORITY

ELECTRONIC LODGEMENT PROJECT

Background

In 1999, the Courts Administration Authority (CAA) commenced a project to enable the electronic lodgement, by legal practitioners, of civil claims forms with the Magistrates Court. The Information Economy Cabinet Committee approved funding for the project budget of $243 000. The initiative offered efficiency gains in administration and processing, resource use and associated costs, to both the CAA and participating legal entities. Cabinet approval was not required for the e-lodgement initiative.

In addition to the electronic form lodgement (e-lodgement) facility, a process was to be developed to enable forms lodged electronically to be accepted for processing directly into the Civil Case Management System (CCMS), CAA's financial and operational system for civil matters. Payment for the e-lodgement service would be made via direct debit or credit card through Bizgate, the Government's electronic payment facility.

The electronic lodgement (e-lodgement) undertaking was a recommendation of the Court Process Review Project in order to improve efficiency and service in the Magistrates Court registries. The e-lodgement project is consistent with the strategic goals of the Authority.

In April 2000, a Project Statement was issued, detailing the project objectives and scope, and the system specifications. It was anticipated that the project would commence with the completion of the Project Statement and would take approximately 12 months to complete, i.e. the project would be completed by April 2001.

An Electronic Lodgement Steering Committee (ELSC) was formed in May 2000, comprising representatives from the CAA and the Department of Administrative and Information Services (DAIS) to facilitate and manage the development of the e-lodgement facility. A Project Team and Legal Reference Group were also established to, respectively, manage external contractors and encourage awareness of the project amongst the legal fraternity (the target external user group).

The tender process began in May 2000 with the issue of a Request for Proposal (RFP) for an e-lodgement solution. The selection process culminated with the execution of the contract with the successful respondent in November 2000.

Over the course of the project, the Project Team met weekly with the external contractors, and formal progress reporting was implemented. The Legal Reference Group, including representatives from the 10 legal firms making the greatest volume of court lodgements, also met regularly to discuss the project's development and to address issues affecting the take-up of the initiative by legal practitioners upon its completion. Both groups reported directly to the ELSC. An independent consultant was engaged to perform a system audit on the e-lodgement facility, including reviews of key documentation, prior to its launch.

The e-lodgement system was officially launched in June 2001.

Audit Focus

Audit's review addressed matters of project management and achievements, and risk management arrangements. Audit gave particular assessment to the adequacy of: business plans; project planning, approvals and management; and monitoring and reporting arrangements.

Audit Findings and Recommendations

Audit's review found that the e-lodgement system was implemented broadly within expected timeframes of just over 12 months, with a cost overrun of approximately $70 000 against a budget of $243 000 and with minimal adjustment to the original scope. Notwithstanding the cost overrun approached 30 percent of budget, Audit was advised that both the Courts Executive and the State Courts Council were forewarned that, due to the nature of the project and inherent uncertainty about actual costs, the project might exceed its initial budget. Budget overruns were approved by the Project Sponsor.

Despite some delays in regular updating of risk assessments, Audit considers that adequate risk management was undertaken. In addition, Audit recognises that seeking an independent security review demonstrated sound project management.

A post-implementation review stated key objectives were met and deliverables were received. Appropriate project management principles and information sharing with key users contributed to the completion of the project. The realisation of benefits by the CAA is expected to occur in the longer term with a target rate of 30 percent of all Magistrate Court lodgements being made electronically. The current rate of use is approximately 10 percent of all Magistrate Court lodgements. However, benefits in terms of efficiency of process and convenience are being realised by the legal entities that choose to make use of the e-lodgement system.

Audit's findings were communicated to CAA in December 2002.

CAA Response *— CAA advised in July 2003 that the Audit findings in relation to the project were noted as consistent, accurate, appropriate and satisfactory.*

Characteristics of Project

In summary, this project has demonstrated the following characteristics:

- Consistency with the strategic goals of the Authority.
- Project milestones were met and objectives achieved with a cost overrun.
- Appropriate project management principles employed.
- Efficiency benefits being realised by users.
- Some uncertainty regarding success of project take up rates with users.
- A 'learnings' report was produced from a post-implementation review.

CHAPTER 5 — AGENCY REVIEW: DEPARTMENT OF EDUCATION AND CHILDREN'S SERVICES

HUMAN RESOURCE MANAGEMENT SYSTEM (HRMS) REPLACEMENT

Background

Previous years Reports have included comment concerning the Department's progress regarding the development of a human resource management system. The project commenced in 1993 and has been suspended several times for various reasons.

In late 1995, a joint development between the then Department for Employment, Training and Further Education, Office for the Commissioner for Public Employment and the Concept software supplier, was established to upgrade Concept functionality to meet the Department needs. In addition to this core development, the Department was also developing, using in house resources, two major systems to integrate with Concept. These systems were a staff entitlement and allocation system and an employment selection and placement system.

In October 2000, a submission from the Minister for Education and Children's Services to Cabinet to complete the implementation of Concept Human Resource Management System and associated systems, at an estimated cost of approximately $16 million including costs incurred to date, was approved.

A joint development contract between the Department and Concept Systems International was signed in October 2001.

Audit Focus

During the year, Audit raised certain matters with the Department of Education and Children's Services (DECS) in respect of the direction of the project development, and other issues relating to funding and costs and project management and reporting.

Audit Findings and Recommendations

The project commenced and was under development for some time prior to the changeover to the current government. Also, since the formation of the current government, significant changes have occurred in respect of the organisation structure of DECS. Changes have involved the separation of the new Department of Further Education, Employment, Science and Technology from DECS on 1 July 2003 and changes in the executive management structure of DECS during 2002-03.

In 1998, an independent review conducted by an external contractor referred to the inadequacy of the project management framework as a major issue impeding effective implementation of the project development and its expected outcomes.

Audit also noted that there have been unsatisfactory aspects over time concerning the matter of project reporting, including on financial reporting on the project development.

In light of the weaknesses noted in project management and reporting for the HRMS development, and the agency and organisational structure changes that may have had implications for the future development of the project, Audit sought clarification regarding project direction and management of its implementation.

DECS Response *— In June 2003, the Chief Executive of DECS advised in writing that a review had been commissioned on the HRMS project relating to its current status. The report was expected to be completed in July 2003 following which an update would be provided to the Minister.*

Audit Review of Commissioned Report

The review report indicated that expenditure on the HRMS Concept development was in the order of $9.7 million as at May 2003.

In addition, the report highlighted a number of problems and risks associated with the project development and implementation process. The more notable of these were:

- Expected implementation of the HRMS across the various staff sectors of DECS was well behind planned timeframes.
- The latest project plan was assessed as ambitious and may not be achieved.
- A potential project budget overrun in the vicinity of $1 million.
- The extent of anticipated savings from implementation of the HRMS of between approximately $2 million to $5 million annually were unlikely to be achieved.
- Undetected bugs in the HRMS Concept software product.

In response to the review report DECS appointed two senior management officers to undertake over six months certain critical tasks. These tasks involve the following:

- Implementation of the Concept system for the Children's Services sector staff of DECS. The current Children's Services system is considered unstable and does not meet legislative requirements.
- Assessment of the capacity, viability and functionality of the Concept system to meet DECS requirements compared with other options for all or part of the DECS workforce.
- Assessment of the budget implications with respect to development, implementation and maintenance for continuing with the Concept system compared with other options.

In respect of the assessment tasks, DECS plans to complete these tasks by late January 2004.

Characteristics of Project

In summary, this project has demonstrated the following characteristics:

- Extensive project delays and extended timeframes for completion.
- Lack of reporting on status of project to Cabinet or the Prudential Management Group.
- Inadequate project management and reporting.

CHAPTER 6 — AGENCY REVIEW: DEPARTMENT OF HUMAN SERVICES

COMPLETE HUMAN RESOURCE INFORMATION SYSTEM (CHRIS)

Background

In April 2001, Cabinet approved the Minister for Human Services to contract with an external service bureau provider (bureau provider) for the provision of a Human Resource Management Service (HRMS) and associated services for the Human Services portfolio at an approved capital cost of $7.6 million.

Cabinet also approved the waiver of tender to allow the Department of Administrative and Information Services (DAIS), on behalf of a number of participating agencies of government, to negotiate with the bureau provider.

The scope of the HRMS functionality includes payroll; leave management; recruitment selection; and training and development. These strategically important projects involve the management of payroll and personnel functions for over 50 000 government employees in over 70 government agencies and health units.

The Department of Human Services (DHS) is responsible for managing the contract and project implementation of the CHRIS HRMS application for the DHS Central Office and all health units. DAIS is responsible for managing the contract and project implementation of the CHRIS HRMS application for a number of participating agencies of government outside the Health and Education sectors.

The following commentary outlines the results of the review by Audit of the DHS implementation. Audit's review relating to DAIS was still in progress at the time of preparation of this Report.

Audit Focus

The Audit review addressed certain project management aspects of the implementation of the CHRIS HRMS application. Audit also examined aspects of the relationship between DHS and the bureau provider and, in particular, the conformance by both parties to the Bureau Services Agreement between the Minister for Human Services and the bureau provider.

In addition, Audit assessed certain key control aspects regarding:

- problem management, change management, user acceptance testing and software configuration release management practices;
- information systems operations;
- Business continuity planning.

Audit Findings and Recommendations

Key findings from Audit's review were:

- The bureau provider had not provided all software modules to DHS, (in particular the leave management, training and development, and recruitment and selection modules), to the level of functionality as contracted.

- Lack of functionality identified in the software had prevented official user acceptance of the software modules by DHS. Issues identified by DHS include the implementation of certain modules of the CHRIS software not finalised which were more than one year later than originally planned.

- DHS and the health units were incurring additional costs in maintaining existing systems while the modules were not implemented and had the potential to incur cost overruns with the retention of the project implementation team longer than planned. Some contract payments were being withheld until a number of matters with the bureau provider were resolved. DHS was actively seeking to manage these issues with the bureau provider.

- The Department and the health units have leave management software operating which had not been officially user accepted by DHS and has software defects. The health units proceeded with entering leave details while accepting advice from the bureau provider regarding future useability of the software and the data. Despite the known defects, the health units had, in effect, accepted the risk of processing with awareness of these defects.

- DHS did not have an overall consolidated system specification from the bureau provider reflecting the details of the current release of CHRIS software. Audit was of the opinion that it is good practice to maintain a complete functional baseline of the system that incorporates changes made to the system.

- Details with respect to agreed payroll processing timeframes in the Service Level Agreement between DHS and the bureau provider differed to actual processing times. This affected planned processing schedules and performance monitoring.

- The Bureau Services Agreement between DHS and the bureau provider did not address some important matters, such as, acceptance testing, change management and variations to initially agreed operating procedures between the bureau provider and the system users.

- While DHS has documented Disaster Recovery Plans, these were not up-to-date or tested.

In October 2003 Audit formally communicated to DHS its recommendations that:

- DHS seek further strategic advice from the Crown Solicitor's Office with respect to finalisation of the implementation of the software modules. Further, Audit was of the opinion that it would be advisable for DHS to inform Cabinet of the status of the project implementation;

- where software versions have been installed which had not been officially accepted by DHS and the health units, the risk inherent in the operation use of this software should be advised to and formally accepted by the health unit or Department Chief Executive;

- DHS review the adequacy of the System Specification in terms of providing a complete functional baseline for the DHS CHRIS system;

- DHS, in conjunction with the health units and the bureau provider, review and agree the 'Payroll Processing Schedule' timeframes and update the 'The Services and Service Level Agreement' to reflect the new agreed timeframes for processing of pay;

- DHS undertake a review of the existing Bureau Services Agreement between the Minister for Human Services and the bureau provider to determine the adequacy and appropriateness of the Agreement. Further, the opinion of the Crown Solicitor's Office should be sought with respect to Agreement terms. In addition, Audit recommended DHS establish mechanisms for regular review of the Bureau Services Agreement to ensure ongoing compliance with the Agreement by both parties;

- with respect to Disaster Recovery Planning, there was a need to review the plans to reflect current circumstances and to schedule plans for testing at the Department's earliest opportunity. Further, DHS should seek a commitment from health units to establish, document and test each Health Unit's Disaster Recovery Plans and maintain that test program;

- DHS undertake a post-implementation review of the DHS CHRIS implementation to identify what has been learned from involvement in this project. Further, DHS should ensure that the results obtained from the review are conveyed within DHS and to DAIS for whole-of-government policy and guidance direction such that lessons/results learnt may be utilised for future projects.

DHS Response *— In response to the matters raised, in November 2003 DHS advised that software modules required to fulfil all contractual obligations continued to be an issue for DHS. Leave management module functionality remained an outstanding item, training and development, and recruitment and selection modules were undergoing acceptance testing, and some software enhancements were being developed. DHS was in communication with the bureau provider management to have this matter resolved. Audit was advised of recent developments where outstanding software modules have been delivered to DHS for testing and acceptance. DHS was considering the recommendation to inform Cabinet of the status of the project implementation.*

With respect to 'leave management' software which had not been officially user accepted by DHS and the health units, DHS advised that neither DHS nor the Health Units believe there was any significant risk in this approach. The response stated that DHS has not accepted the CHRIS leave modules and this had been reinforced by DHS withholding milestone payments to the bureau provider. In response to the recommendations by Audit, DHS would formally communicate to all Health Units regarding the risk of operating the yet to be finalised CHRIS leave module and seek their acceptance of the risk.

DHS advised that it did not agree with Audit comment in relation to the absence of a comprehensive, detailed system specification against which to compare baseline functionality of the CHRIS system. In response to the recommendations by Audit, DHS would review the adequacy of the system specification. Following that review, DHS would agree the nature and content of the system specification with the bureau provider and if necessary, arrange for appropriate variations to the current Bureau Services Agreement to reflect this new understanding. The bureau provider would then be requested to provide an up-to-date System Specification and to maintain its currency.

In other matters, DHS stated that Health Unit and DHS Central sites were verifying alignment of existing processing schedules with the bureau provider.

DHS had spoken to the Crown Solicitor in relation to commencing a review of the Bureau Services Agreement and its terms as a matter of urgency.

In regard to Disaster Recovery Planning, DHS advised of revision and update of certain Disaster Recovery Plans and of testing that was planned or had taken place. The issue of Health Unit site's outstanding Disaster Recovery Plans had been escalated to governance committees and user groups in October 2003.

DHS stated that it would undertake a Post-Implementation Review of the HRMS Project approximately six months following the end of the implementation phase with the results and findings of the review communicated to DHS, the Health Units and DAIS for reference in future projects.

Characteristics of Project

In summary, this project has demonstrated the following characteristics:

- Contractor unable to deliver all software modules to acceptable functionality on time as contracted.
- Project delay and extended timeframe for completion.
- Contract milestone payments withheld.
- Additional costs borne by DHS and health units in maintaining existing systems.
- Certain software modules installed in production prior to formal acceptance by DHS.
- Business continuity and disaster recovery testing not completed.
- Lack of advice to Cabinet of significant change in status of projects or periodic status reports.

OPEN ARCHITECTURE CLINICAL INFORMATION SYSTEM (OACIS)

Background

The Open Architecture Clinical Information System (Oacis) system was designed to provide computer based integrated clinical information. Oacis Healthcare Systems Corporation developed the system which is used by a number of United States hospitals and health bodies.

The Oacis system stores in electronic form certain information relevant to the clinical care of patients. It is not a complete electronic patient record because it does not include all the information that may be found in a patient's medical record. However, it provides the platform for a comprehensive electronic patient record in the future.

The Oacis system was installed in 1997, as a pilot, within the renal units of the North Western Adelaide Health Service (The Queen Elizabeth Hospital), Royal Adelaide Hospital, Women's and Children's Hospital and Flinders Medical Centre.

Approval was given in 2000 for the continuation of the implementation and use of Oacis within the renal units of the above-mentioned health units, and to extend the rollout of Oacis, as the common clinical information system, to include all other clinical disciplines within those health units and other nominated hospitals, namely, North Western Adelaide Health Service (Lyell McEwin Health Service), Modbury Public Hospital,

Noarlunga Health Services and Repatriation General Hospital at a total estimated project cost of approximately $87 million. The Cabinet and DHS approved amounts for the project since inception totals approximately $115 million.

It is anticipated that there will be approximately 10 000 clinical users of the Oacis Clinical Display and Clinical Order Management modules across the eight health units. Audit has been advised by DHS that the extension of the modules into the 8 health units should be implemented by June 2005.

At the time of preparation of this Report, Oacis included patient demographic data, laboratory and radiology results, outpatient bookings, and summary information about inpatient admissions, including final diagnosis. DHS envisaged summary information about emergency department visits and operating theatre episodes would be added in 2003.

Using Oacis, clinicians can view and sort information and chart test results. Renal physicians can also add information to Oacis regarding the care and treatment of renal patients via purpose developed data collection screens. The screens were developed during the initial pilot project in the renal units. The screens enable the capture of renal dialysis information, pharmacy information, outpatient consultations and other related information.

Three private renal dialysis units have an involvement in the Oacis programme. A deed of confidentiality between the Minister for Health and each private renal dialysis unit has been prepared.

At the time of this review, Audit was been advised that there was no intention to extend the Oacis programme beyond the public hospitals. There is, however, increasing pressure to extend access to the Oacis system into the private sector and should that eventuate, Audit notes that certain legal risks and privacy issues would take on increased importance.

Also at that time, Audit was advised that the Oacis Clinical Display module implementation to seven of eight health units was substantially completed and that the Clinical Order Management module is in pilot operation at the Royal Adelaide Hospital and the Lyell McEwin Health Service. Approximately 9500 users have been trained to date. Post-implementation reviews of the Clinical Display implementation and Clinical Order Management pilot were expected to be completed in early 2004.

The Oacis programme is a major initiative of DHS and government. The programme will give the metropolitan public hospitals a uniform clinical information system for the management of patient care and provides the platform for a comprehensive electronic patient record.

Audit Focus

Audit's review addressed certain aspects of the Oacis programme relating to project management, achievements and risk management arrangements, including business plans, project planning, approvals and management and monitoring and reporting arrangements.

In addition, although Audit has been advised that there was no intention to extend the programme beyond the public hospitals to general practitioners and private hospitals, in

its review Audit considered the legal implications of private healthcare providers being involved with the system.

Audit considered it relevant to consider the involvement of private entities such as general practitioners and private hospitals for two reasons. Firstly, three private hospitals are involved in the renal project. Secondly, Audit has been advised by DHS that there has been some pressure from other sources including the medical profession to expand the programme scope beyond the current public sector use.

Audit Findings and Recommendations

At the time of preparation of this Report, reported costs of the programme from inception in 1995 to October 2003 were in the vicinity of $85 million against a total approved value of approximately $115 million. Despite some identified delays within the programme, Audit was advised that the variations will be accommodated within the programme timeline and will not affect the proposed completion date of 30 June 2005. It was also advised that the variation would be accommodated within the current approved funding level.

Programme costs are captured and reported in a disciplined manner and meet forecast values. Considering the importance, financial magnitude and extended duration of the programme, and pressures from various health units and the medical profession for inclusion of additional scope within the programme, Audit recommended that the programme continue to be closely monitored to minimise any potential time and cost overruns.

Audit notes the proposed completion date for the Oacis programme of June 2005. With respect to current pressures to extend access to the Oacis system to other health units and the private sector, Audit considered that the future feasibility and strategic direction for the expansion of the Oacis programme for 2005 and beyond should be assessed and endorsed by DHS management and government.

Audit considered it important that DHS continues to maintain regular risk management assessment of the programme.

In summary, Audit considered that project management for the Oacis programme is conducted in a disciplined manner.

Given the significance to the health sector and the size of this initiative, Audit considered it important that commentary with respect to the Oacis programme be included in the DHS Annual Report. Such reporting is also envisaged under the Annual Reporting Requirements issued by the Department of Premier and Cabinet.

Audit's findings were communicated to DHS in February 2003.

DHS Response *— DHS advised in March 2003, it was reassured by Audit's findings with regard to the project management component of the Oacis Programme. Given the importance, financial magnitude and the pressure applied from various health units and the medical profession to expand the scope of the programme - the need to continually monitor the programme's progress is paramount.*

In addition, the Department advised that it would include specific commentary with respect to the Oacis Programme in the upcoming Departmental Annual Report.

Audit conducted a follow up review in September/October 2003 and sought an update on the future direction of the programme.

DHS further advised in September 2003 that:

- *the programme remains on track within the nominated completion timeline of June 2005 and the current approved funding level;*

- *a DHS commissioned project implementation review of the programme conducted by an independent external consultancy was underway and was expected to be completed by the end of October 2003;*

- *DHS have sought Crown Solicitor's Office involvement for legal considerations with potential commercialisation and intellectual property transfer arrangements of DHS developed software enhancements to the Oacis software owner;*

- *the scope of the Oacis programme remains unchanged. DHS anticipate commencing discussions in early 2004 regarding expansion and funding continuation for 2005 and beyond.*

In November 2003 DHS further stated that, at this stage, there is no intention to extend Oacis beyond present arrangements.

In addition, DHS advised that it is anticipated that the DHS commissioned project implementation review of the Oacis Programme would be available in November 2003.

Characteristics of Project

In summary, this project has demonstrated the following characteristics:

- Project management for the Oacis programme is conducted in a disciplined manner.

- The programme remains on track.

- A revisit of the future strategic direction may need to be undertaken to provide extended use of the Oacis system facilities.

CHAPTER 7 — AGENCY REVIEW: DEPARTMENT OF TRANSPORT AND URBAN PLANNING — TRANSPORT SA

ELECTRONIC COMMERCE FACILITIES FOR REGISTRATION AND LICENSING

Background

Transport SA (TSA) and EDS (Australia) Pty Ltd (EDS) have developed an e-commerce service for a range of motor vehicle registration and driver licensing transactions. Cabinet approval was given in July 1998 and a New Services Agreement was signed with EDS in October 2001.

The project was expected to cost in the vicinity of $12.9 million over an eight year period. The development of electronic commerce facilities for registration and licensing transactions contributes to the Government's objective to provide the public with efficient and effective access to information and transactions processing through a secure electronic system.

The system includes access via the Internet and use of an interactive voice recognition facility. TSA considered the development of an e-commerce facility to be outside its core business and so the project was developed on the basis that EDS build, own (or lease), operate, manage and maintain the system.

Because of delays in progress during the development stage, TSA sought certain advice and clarification in respect of the contract arrangements in proceeding with the contract.

The services are provided by EDS on a fee per transaction basis with TSA having no liability for the cost of development and operation of the system. EDS own the intellectual property associated with the e-commerce system and the company plans to commercialise it. Material supplied or created by TSA for the system remains the property of the Department.

The new TSA e-commerce system makes available 25 types of transactions to be conducted via the Internet. These include; registration quotes and renewals; modification of registration details and transfers; licence details and driver offence history enquiries; and enquiries and the recording of interests for the vehicles securities register. Transactions requiring payments are payable by credit card or direct debit. Audit has been advised that agreements with financial institutions have been finalised to implement these payment systems. An implementation and maintenance contract was formally executed with EDS in June 2003 with finalisation of the development of the 25 transaction types.

Audit Focus

Audit's review essentially addressed matters of project management and achievements and risk management arrangements. Audit gave particular attention to the adequacy of business plans; project planning, approvals and management; and monitoring and reporting arrangements.

Audit Findings and Recommendations

Audit notes that TSA sought to reduce the risks to government by engaging an external service provider (EDS) to build, own (or lease), operate, manage and maintain the system.

In July 1998, Cabinet gave approval for TSA to establish electronic commerce facilities and approved an increase of $1.5 million in capital forward estimates for TSA to fund this initiative.

Despite an extended period of time between the original Cabinet approval in July 1998 and the signing of a New Services Agreement with EDS in October 2001, the deliverables although modified in scope, were completed with all transaction types available in June 2003.

Audit's review revealed a delay during the development stage of the project that resulted in a slippage from the target completion date of late 2002 to mid 2003. With respect to the project delays, Audit notes that further slippage would have presented a risk to identified future TSA dependent projects, notably DRIVERS replacement system, Transport User Management Processing System (TRUMPS).

Audit was advised that, in December 2002, the TSA cost to date for the internal development and implementation was approximately $1.6 million against the Cabinet approved funding of $1.5 million.

As TSA project costs are predominantly salary based, taking into account the project delay, it is likely the project would be subject to over-expenditure against original funding allocations. Although the project is funded within the existing TSA budget, Audit recommended that management clarify and document the forecast project cost, and confirm that remaining funds are sufficient to meet project completion by the due date, for presentation to and management by the Electronic Commerce Sponsor Group.

Audit considered the Prudential Management Group should be updated in terms of the project development status.

Audit's review has highlighted a need for tight control over project costs and costs monitoring and the increased need for prudent risk management in relation to identified risks. Audit recommended that the project continue to be closely monitored and corrective action applied where necessary to minimise project time and cost overruns. In this regard, Audit considered that:

- aspects of the TSA internal development methodology, namely the development of the Project Management Plan and formal endorsement and approval of phase end reports need to be undertaken. Audit believes there are opportunities for improvement with the presentation of ongoing formal project status reports to governance committees;

- regular risk assessments need to be conducted, mitigation strategies identified and the findings documented as part of normal management of the project;

- a benefit realisation measurement system be implemented and that TSA undertake periodic reviews of the proposed benefits throughout the development and implementation of the project.

Audit communicated the findings and recommendations to TSA in December 2002.

Transport SA Response *— In March 2003, TSA advised that it had implemented a full review of the Registration and Licensing E-Commerce Project in early 2003, in conjunction with the Department of Treasury and Finance. The project was not changed as a result of the legal advice sought.*

In September 2003, Audit conducted a follow up review and sought an update on outstanding matters in relation to the project.

In September 2003, TSA advised that the eight year contract with EDS was formally executed in June 2003. A high level Governance Committee had been established to monitor the contract and make any recommendations that may be necessary to ensure Government's interests are maintained and that the savings to Government are maximised.

The indication from analysis of the e-commerce transactions which have already occurred, is that the number of transactions is already in excess of the minimum floor limit hence the overall savings are likely to be greater than the business case suggestions.

With respect to revisiting the business case, independent advice was sought after consultation with the Prudential Management Group about the assumptions in the business case.

Had the Business Case or independent review shown an adverse impact to the projected savings, the issue would have been appropriately documented and referred back to Cabinet.

TSA stated that processes were enhanced by the seeking of advice from the Crown Solicitor's office and from independent reviewers and experts at key stages during the project.

A Post-Implementation Review report was scheduled for completion in October 2003.

Characteristics of Project

In summary, this project has demonstrated the following characteristics:

- A long term contract (eight years) for over $12 million with EDS.
- Development of 25 transactions types providing an e-commerce service for motor vehicle registration and licensing.
- Project delays and extended timeframes for completion.
- Lack of timely advice to Cabinet or the Prudential Management Group of significant change in the status of project or periodic status reports.

CHAPTER 8 — AGENCY REVIEW: DEPARTMENT OF TREASURY AND FINANCE — REVENUESA

REVNET PROJECT

Background

RevenueSA (a branch of the Department of Treasury and Finance) is responsible for the collection and enforcement of the State's taxation revenue base. This includes a range of licence fees, stamp duty, payroll tax, land tax and the fixed property component of the emergency services levy. In 2002-03, the revenue collected in relation to these tax bases was over $1.9 billion.

The RevNet electronic lodgement facility is a major initiative of RevenueSA. The project is one that is in line with the government thrust for provision of alternative payment and lodgement facilities via the Internet.

In April 2001, the Department of Treasury and Finance identified the replacement of the existing 'TIMBER' system as a critical aspect in minimising risks and ensuring the collection of the State's revenue was not compromised. The Department provided funding of $1 million from the 2001-02 budget for the development of RevNet. The RevNet project is a component of the RevenueSA Information Systems to Enable Compliance (RISTEC) initiative, for which funding of $22.6 million, over four years, was approved by Cabinet in 2002.

RevNet is an electronic lodgement facility for RevenueSA clients to self-assess, pay for and stamp documents attracting stamp duty. This core functionality is also extended to provide for the online request and delivery of Agent Certificates for Emergency Services Levy and Land Tax, and payments of Search Request Fees and Certificate Liability.

The development and implementation of RevNet was to occur incrementally in three phases and was expected to be completed in mid 2002.

Audit Focus

This review addressed matters of project management and achievements, and risk management arrangements for the RevNet project. In particular, Audit assessed the adequacy of:

- Business plans
- Project planning, approvals and management
- Monitoring and reporting arrangements.

Audit Findings and Recommendations

Audit found that certain elements of planning and project and risk management were in place for the project.

Regarding progress, the first two planned phases of the project have been completed with slippage of approximately nine months from the original timeframe estimates. The final phase was completed in 2003.

Audit was advised that the project adopted a risk management approach by deferring development while evaluation of feedback from participants of a pilot implementation was assessed. This resulted in modifications and enhancements which extended the implementation dates. Audit's review of RevNet Project Steering Committee minutes confirmed that the slippage was reported to and monitored by the Committee. Audit was advised that a Post-Implementation Review would be conducted at the conclusion of the project.

Review of RevNet Project Steering Committee minutes revealed, however, no evidence that the Committee was monitoring project expenditure against budget. The Terms of Reference for the Steering Committee did not make specific reference to this aspect. Discussion with the Department revealed that the Assistant Commissioner, Revenue Business Services, is responsible for the financials of the project.

Audit would expect that the Steering Committee would be appraised of project financials to ensure the overall effectiveness of the governance role of the Committee. Audit recommended that management reviews the roles and responsibilities of the Committee with respect to financial monitoring and reporting for the continuation of this RevNet project and for the overall RISTEC project.

Actual project expenditure for the period ending January 2003 was approximately $955 000 against the project budget value of $1 million. As the project costs are predominantly salary and contractor expense based, the project is likely to be subject to some over-expenditure against original funding allocations. At the time of the review, Audit recommended that the project continue to be closely monitored and any corrective action applied where necessary to minimise project costs overrun.

In respect to planned achievements, Audit found no formal documented benefit realisation measurement system which was regularly reviewed in place for the RevNet project. Establishment and monitoring of a project benefit realisation measurement system helps reduce uncertainty with the expected benefits being achieved. At the time of the review, Audit recommended that a benefit realisation measurement system be implemented to provide specific quantifiable measurement, particularly for the planned post-implementation review. Further, Audit recommended that future RevenueSA projects include such measurement systems as part of the project methodology.

Audit communicated the review findings to RevenueSA in April 2003.

Department Response *— In May 2003, RevenueSA advised Audit that it agreed with the summary findings with some clarifications. RevenueSA advised that whilst the Terms of Reference for the Steering Committee do not make specific reference to the monitoring of Project expenditure, this aspect was reviewed at a RevenueSA senior management level via standard RevenueSA expenditure review mechanisms. With regard to benefit realisation measurement systems, RevenueSA advised of specific identified benefits.*

Audit conducted a follow up review in September 2003 and sought an update on the status of the RevNet project.

In November 2003, Audit was advised that in relation to the RevNet project:

- *the RevNet project was completed in June 2003 with software releases now being undertaken;*

- *separate project funding of $400 000 was allocated for functionality under RevNet for payroll tax annual reconciliation over the Internet and this is expected to be competed during this financial year;*

- *the project expenditure came within the budget of $1.4 million for both projects;*

- *a post-implementation review of the RevNet project will be commenced within the 2003-2004 financial year;*

- *the RevNet Steering Committee meetings are aligned with project milestones, generally every 3 months;*

- *aspects of a Benefits Realisation Measurement system will be conveyed to the RISTEC Project Director for consideration.*

Characteristics of Project

In summary, this project has demonstrated the following characteristics:

- Specific identified benefits achieved.

- Certain elements of planning and project and risk management in place for the project.

- Project completion within budget.

- Some project delay and extended timeframe for completion.

- Importance of formal benefit realisation measurement systems.

CHAPTER 9 — AGENCY REVIEW: DEPARTMENT OF WATER, LAND AND BIODIVERSITY CONSERVATION

WATER INFORMATION AND LICENCE MANAGEMENT ADMINISTRATION SYSTEM

Background

In May 2001 Cabinet approved the development of a new water licensing system, Water Information and Licence Management Administration System (WILMA), to support the administration of the *Water Resources Act 1997* and to enhance state economic development through the facilitation of trading of water allocations and salinity credits.

Capital funding approved through Cabinet for this project was $3.3 million. A contract was awarded to an external system developer in November 2001 with a specified completion date of October 2002. The total contract price for software application development and licensing was $1.4 million.

During the development phase in June 2003, a number of key project positions were terminated or vacated and an independent consultant was engaged for a review of the project as a result of concerns over delays in project delivery. The project had not been finalised at the time of preparation of this Report.

Audit Focus

The review addressed matters of project management and achievements and risk management arrangements. Audit gave particular attention to the adequacy of project reporting and project assurance and the future direction/status of the project.

Audit Findings and Recommendations

As at June 2003, the total expenditure incurred for the project was $1.9 million (including progress payments of almost $1 million to the system developer).

With respect to progress, the minutes of the Project Board provided limited commentary on the overall progress of the project. Moreover, the minutes did not indicate the circumstances leading to the termination of key project positions and the appointment of an independent consultant engaged for review of the project.

Audit considers adequate reporting a critical aspect of managing and accounting for any major project and its related expenditure. It was subsequently recommended that the Department establish an appropriate reporting framework.

A Project Board endorsed 'Roles and Responsibilities of Project Board, Project team and Reference Group' document refers to a project assurance function providing the independent monitoring of all aspects of the project's performance and deliverables including ensuring that risks are being controlled. Audit found no evidence that this function was being performed as intended. Audit recommended that the responsibilities of this project assurance function be formally assigned to appropriate officers.

In general, Audit found that key milestones in the delivery of the project had been delayed significantly and there were, at the time of the audit, a number of unresolved issues surrounding the functionality of the system.

In June 2003, as a result of concerns over delays in project delivery, the Department of Water, Land and Biodiversity Conservation (DWLBC) appointed an independent contractor to conduct a major review of the WILMA project. Coinciding with the review process, a number of key project positions were terminated or vacated.

The future direction of the project and the appointment of officers to key project positions were deferred until the completion of the independent review. As at July 2003, a revised completion date had not been agreed with the provider.

The report of the independent review conducted in July 2003, concluded that 'unless significant and immediate corrective action is taken the WILMA project is at high risk of non-completion within its existing budget.' The main sources of concern for the project presenting the most risk were detailed as:

- business requirements have not been adequately reflected in the formal documentation provided throughout the project;
- contract terms and conditions are not currently favourable for timely implementation of a satisfactory system;
- project and relationship management is currently not conducive to collaborative corrective action.

The independent review report recommended that the Department 'develop and agree a detailed project plan for completion including costs and methods' to be used 'as the basis for a decision whether to proceed or not and under what conditions.'

In August 2003 the independent reviewer was awarded a contract regarding services for WILMA project viability and management including the development of a project implementation plan.

DWLBC Response *— In August 2003 the Department advised it had introduced monthly WILMA Project Board reporting to DWLBC Executive and has encouraged greater recording of commentary on decisions made during their regular meetings.*

With respect to project assurance, the Department considered that Board members could provide the necessary independent monitoring required and that project assurance was implemented to a reasonable degree through:

- *management and executive liaison with the Contractor;*
- *user representation on the Board and general consideration at Board meetings;*
- *management and executive input and consultation;*
- *general consideration of risks at Board meetings including a number of specific agenda items.*

Notwithstanding this, the Department advised of their intended adoption of more formal processes through the engagement of an independent contractor to assist in monitoring and addressing project risks.

Characteristics of Project

In summary, this project has demonstrated the following characteristics:

- Project delays and extended timeframes for completion.
- Inadequate reporting of significant change in the status of the project.
- Risk management arrangements not performed as intended.
- Proactive intervention by management for project reassessment.

PART 3 — IT SECURITY AND CONTROL

PART 3 — IT SECURITY AND CONTROL

TABLE OF CONTENTS

PART 3 — IT SECURITY AND CONTROL

TABLE OF CONTENTS

CHAPTER 10 — REVIEW BACKGROUND AND KEY FINDINGS AND COMMENTS

BACKGROUND

Introduction

There is a wide and diverse range of agencies that are dominant users of IT that operate across the public sector in South Australia.

The public sector IT arrangements are characterised by large outsourcing contracts with the private sector, including the provision of government IT infrastructure, communications, and radio networks and key government-wide financial systems for accounts payable, accounts receivable and human resource management systems. Individual agencies in their own right are also responsible for the development of a significant range of diverse systems over many major areas of Government service delivery and financial operations.

The effective management, security and control of agency systems and computer processing environments is essential for the completeness, accuracy and integrity of financial record keeping and financial statement production as well as the achievement of government and agency operational objectives. These management and security control arrangements are essential components for the ongoing continuity of business operations and the protection of agencies information and assets.

This Part of this Report presents the findings from Audit reviews of some key aspects of IT Security and Control of selected agency/entity systems and computing environments.

Audit Mandate

The Audit review process was conducted pursuant to section 36 of the *Public Finance and Audit Act 1987.*

Government Mandated IT Security Requirements

In April 2003, Cabinet approved the adoption of the SA Government Information Security Management Framework (ISMF), as the current information technology security standards and guidelines for implementation by agencies in this State. In accordance with this approval the Major Projects and Infrastructure Cabinet Committee is authorised to approve future versions of the ISMF, and any associated standards, procedures, work practices and guidelines.

The ISMF represents an alignment with international information security standards being adopted by all Australian Governments and provides for a consistent approach for all South Australian Government agencies in protecting business operations.

The ISMF will be introduced through a program of work including, a transition guide from current standards and guidelines, provision of agency security awareness training and the integration of new security work practices. Implementation of the overall project is estimated to cost in the vicinity of $1.3 million over four years.

The ISMF, when fully implemented will replace the Government's 'Information Technology Security Standards - In an Outsourced Environment' that was promulgated in 1994.

AUDIT REVIEW

The Auditor-General's Department audits in excess of 160 public sector entities, including administrative agencies of government, health units, and other public sector entities. This Part of this Report examines the activity undertaken in respect to IT systems, facilities and operations at a selected number of those entities.

Audit's reviews examined some key aspects relating to the following matters:

- strategic planning for IT
- business continuity planning
- operating procedures for systems and facilities
- formal arrangements with the private sector for IT service provision
- security policies and procedures
- access to systems and information
- implementation and maintenance of systems and facilities.

The reviews of systems and computing environments have essentially been undertaken against the Government mandated security control requirements promulgated in December 1994, supplemented by more current better practice procedures in management and control of IT systems and facilities.

AGENCIES REVIEWED

The specific reviews of agency/entity computing facilities and systems undertaken by Audit during 2002 and 2003 and commented on in this Part of this Report, cover the main industry/operational areas of government. They demonstrate the magnitude and significance of Information Technology developments and their contribution to the service delivery outcomes of government and the agencies/entities concerned.

A brief summary of the areas reviewed are described hereunder.

Education Sector

The main school administration system for managing student records, financial transactions, funding information and provision of reporting to the Department of Education and Children's Services (DECS) head office is the Education Department School Administrative System (EDSAS). This is a key financial and operational system used throughout approximately 600 State schools. 10 specific schools were selected in conjunction with DECS as a representative sample. Those schools and the DECS head office were reviewed by Audit.

The Senior Secondary Assessment Board of SA uses a students results processing system to provide the academic results for over 20 000 students throughout the State and the Northern Territory. These results provide the basis for University entrance offers made to those students in the following year. The students results processing system and computing facility was reviewed by Audit.

Audit also reviewed the communications network and computing facility which provides remote access to certain financial and operational systems and facilities of the University of SA. A particular focus of the review was to ascertain the extent of adequacy of the relevant controls concerning the Finance and Human Resource Management systems and to identify improvements to the control environment if appropriate.

Health Sector

The computing facility and network which supports the operation of the State's primary patient clinical management system (Oacis), falls under the responsibility of the

Department of Human Services. Oacis is a clinical information system which provides real-time integration of patient information from multiple administrative and specialist clinical departmental systems. Oacis is a major initiative of the Department of Human Services and government. The computing facility and network was reviewed by Audit.

Audit also reviewed key computing facilities at three major health units, ie the Flinders Medical Centre, North Western Adelaide Health Service and the Royal Adelaide Hospital. These health units are major health service providers and are significant users of Information Technology. This technology is important to the operations of the health unit business and service delivery outcomes.

Justice Sector

The SA Police Department uses a key system for the capture of traffic infringements and raising of expiation notices for the associated fines. The system referred to as CARS has been developed under arrangements with an external contractor to provide computerised film scanning, adjudication, archiving, document management and reporting services and to incorporate technologies such as digital film processing and optical character recognition. During 2001-02, in excess of 300 000 notices were issued with a value of more than $49 million. The computing facility and system was reviewed by Audit.

EDS at its Glenside processing bureau manages certain computing facilities which support the processing of a key system used by justice agencies (Justice Information System), and certain other systems for the Courts Administration Authority. These systems provide for sensitive operational justice related information and the processing of financial transactions essentially for raising of fines. Audit reviewed those computing facilities and aspects of the management and control arrangements in place at the justice agencies concerned.

Gaming Sector

The central system operated by the Independent Gaming Corporation Ltd is used for monitoring and recording of the activities of approximately 15 000 gaming machines. Those gaming machines are located in approximately 600 individual venues and clubs in the State. Operation of the gaming machines contributes millions of dollars to the State's revenue base. The facility and system was reviewed by Audit.

Government-Wide and Other Reviews

A government-wide CHRIS Human Resource Management System has been implemented for public sector agencies and health units. This is a major outsourcing arrangement for the provision of payroll and personnel functions for over 50 000 employees in over 70 government agencies and health units. This system is managed by a private sector bureau service provider.

Audit sought to determine the adequacy of controls over the outsourced computer processing facilities.

The Department for Administrative and Information Services (DAIS) outsourced provision of a major inventory management system and computing facilities to an external bureau service provider. The system processes the procurement of inventory on behalf of government agencies, statutory authorities, charitable organisations, public and private schools, and health units. DAIS services over 3000 customers covering the State of South Australia and parts of the Northern Territory. That outsourced arrangement and the computing facilities were reviewed by Audit.

Audit also reviewed key computing facilities for the Department for Environment and Heritage (DEH) and the Department of Primary Industries and Resources (PIRSA).

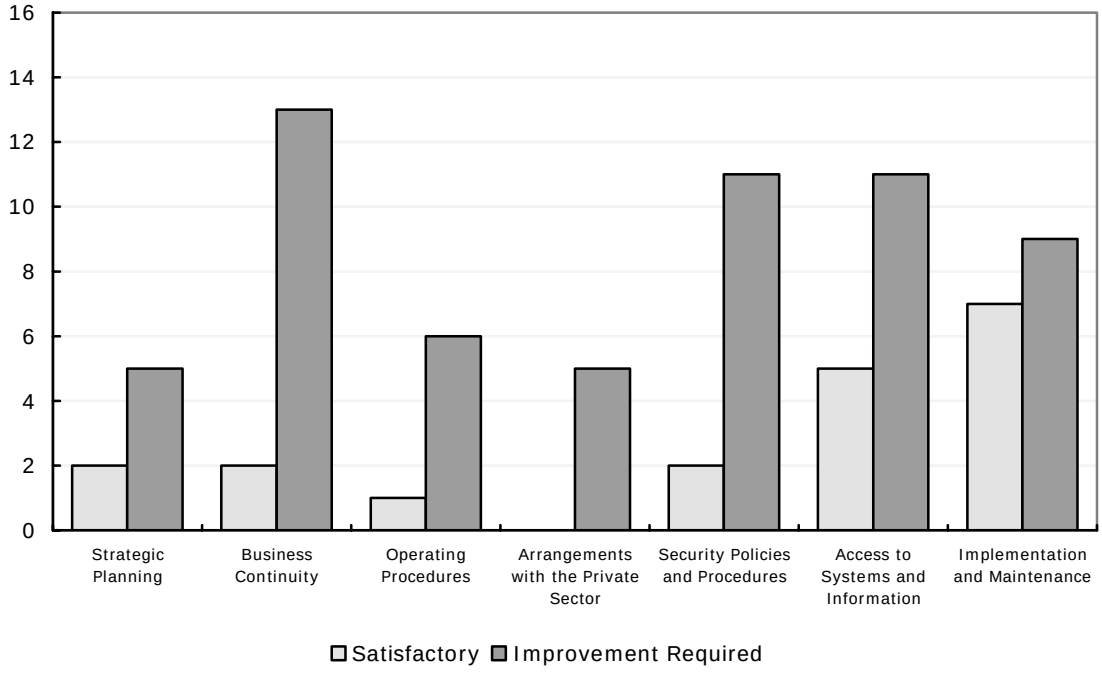
KEY AUDIT OBSERVATIONS

The outcome of agency/entity reviews identified both good practice in management and control, and some examples of inadequate security control and management deficiencies. The main or more common deficiencies emanating from the reviews were:

- Inadequate attention to strategic management and planning for IT.
- Lack of up-to-date, documented and tested arrangements for continuity of business operations.
- Unsatisfactory formal agreements with the private sector for IT service provision.
- Need for improvement in documented security and operational policies and procedures.
- Inappropriate access provided to users to systems and information.

Audit also found instances of weakness in the provision of user training, a need for revision and formal documentation of high level business risk assessment and management, and inadequacies in monitoring of system use and security logging.

The following diagram provides a broad illustrative example of the extent of occurrence of these weaknesses in the agencies reviewed in 2002 and 2003.



In interpreting this bar graph, it is necessary to understand that not all control areas were examined in all agencies. For this reason, each control area is representative of only those controls examined by Audit. The indicative trend that is illustrated by the graph is that in all control areas there are inadequate management control practices.

All reviews were the subject of formal audit management letters to the agencies/entities concerned and responses indicating corrective action have been received in all cases.

INDIVIDUAL AGENCY REVIEWS

Specific agencies and IT Project developments reviewed and commented on in the following Chapters of this Part of this Report are:

Department for Administrative and Information Services	Inventory Management System Three EDS Glenside Managed Environments
Department for Administrative and Information Services and Department of Human Services	Complete Human Resource Information System (CHRIS)- Government-Wide
Department of Education and Children's Services	Education Department School Administrative System
Department for Environment and Heritage	Computer Processing Environments
Health Units	Three Certain Computer Processing Environments
Independent Gaming Corporation Ltd	Gaming Machine Monitoring System
Department of Primary Industries and Resources	Computer Processing Environments
Senior Secondary Assessment Board of South Australia	Results Processing System
South Australian Police Department	Capture Adjudication and Reporting System
University of South Australia	Remote Access Facility

The reviews presented examine IT security and control measures taken by government and agencies to mitigate risks, including those previously identified by Audit. The focus is on matters of a security and control nature.

CONCLUDING COMMENT

Government Security Requirements

Inadequate security and integrity weaknesses exist in certain agency IT systems and computer processing environment operations. The weaknesses identified by Audit, in general, reflect non-compliance with government mandated security standards by agencies.

New standards are being introduced by government to address the current requirements of information security. As mentioned above, this is through the promulgation of the new Information Security Management Framework. It is also proposed to have a formal education program to ensure that all agencies are fully aware of the new standards and how to apply them.

Contracts with the Private Sector

There has been ineffective management control exercised by government agencies in some contracts with the private sector.

Agencies need to actively manage the relationship with outsource service providers and ensure the formal contract arrangements provide adequate security and protection and

that the security requirements can be effectively monitored and reviewed by Government.

This is particularly relevant at this time as the Government is preparing to enter into a series of new arrangements for IT infrastructure provision and services for the future. In so doing, it is reviewing many of its existing whole-of-government and large IT contracts.

Risk Management Practices

Some Government agencies' risk management practices have not been adequately established. Others are not revisited on a regular basis as may be necessary.

It is important that agencies adopt appropriate risk management regimes which are regularly revisited, particularly in areas such as purchasing of IT services, operations management, the protection of information assets, and business recovery arrangements.

CHAPTER 11 — AGENCY REVIEW: DEPARTMENT FOR ADMINISTRATIVE AND INFORMATION SERVICES

INVENTORY MANAGEMENT SYSTEM

The Department for Administrative and Information Services (DAIS) through its contract services branch, is responsible for the procurement of inventory on behalf of government agencies, statutory authorities, charitable organisations, public and private schools, and health units. DAIS services over 3000 customers covering the State of South Australia and parts of the Northern Territory. Warehouses are situated in Adelaide and Whyalla with an average inventory value of $2.2 million which doubles over the 'back to school' period. Inventory held principally includes stationery, office supplies and equipment, medical and occupational health and safety products, hardware, and cleaning materials.

Key aspects of the inventory warehousing and logistical operation have been outsourced to an external bureau. The bureau operates a Unix computer processing environment, supporting an inventory warehouse management system. The system comprises a series of financial modules and information in respect of inventory held by Contract Services. The information is updated from Contract Services head office and regional areas, with the physical control and responsibility of inventory and computer processing environment operations performed via the external bureau.

At the time of preparing this Report, the system was being brought back under DAIS management.

Audit Focus

Audit undertook a review of the inventory management system and control aspects of the external computer processing bureau managed by the private sector IT service provider. Audit's review entailed examination of the following matters:

- DAIS Security Policy and supporting procedures, including contract arrangements between DAIS Contract Services and the private sector IT service provider.
- Security control arrangements of the inventory system, including database security controls.
- Network security controls.
- Controls supporting the operating systems security and configuration.

Audit Findings and Observations

A number of important areas were identified in need of management attention to effect required control improvements and these were communicated to the Department in August 2002.

Some of the more salient matters requiring control improvement included:

- formalisation of a Service Level Agreement between DAIS Contract Services and the private sector IT service provider for the IT infrastructure services;

- addressing numerous technical exposures on the Unix internal network computers, the system software security configuration of the computers; and the system administrator personal computer;

- development, implementation and testing of a business recovery plan and a business contingency plan;

- formalisation of backup procedures and backup logs.

DAIS Response *— DAIS advised in August 2002 that the existing arrangements for warehousing and distribution between DAIS Contract Services and the private sector IT service provider were under review. A Cabinet submission recommending a future strategy for the warehouse was being processed. A project plan and project team has been established to immediately address the matters identified as high risk. Implementation of the remaining recommendations would be subject to the outcome of the review.*

Audit conducted a follow up review of the above findings and response in October 2003.

DAIS advised in October 2003 that a transition contract between the private sector IT service provider and the SA Government had been formalised. The software developer has agreed to assign the software licence to the government and this agreement is currently being formalised.

DAIS advised that the first stage remedial work to address high-risk exposures on the Unix network computers, the system software configuration of the computers and the Administrator personal computer was completed in July 2003 by an external security contractor. The subsequent stages of remedial work required reassessment given the unresolved decisions regarding IT infrastructure.

The action to be taken on other outstanding issues had been dependent on decisions made in relation to the in-sourced warehouse agreement which had now been resolved and work was proceeding on the development of the following:

- *Problem escalation, application, system and network policies and procedures.*
- *Business recovery plan.*
- *Business contingency plan.*

SELECTED EDS GLENSIDE MANAGED ENVIRONMENTS

EDS is principally responsible for the processing of public sector financial and operational systems at its Glenside site, including certain mandated whole-of-government financial systems under contracted arrangements with the State Government. EDS operational controls are of primary importance in ensuring that Government systems are secure when resident on EDS's infrastructure.

Audit Focus

To enable Audit to form an opinion on the adequacy of the controls within EDS's managed environments, focused reviews of selected aspects of EDS operations have been undertaken since introduction of the IT Infrastructure outsourcing arrangements with the Government.

Audit undertook a review of EDS Glenside site selected EDS managed environments. That review covered aspects of the Department of Human Services (DHS), Justice Technology Services (JTS) and the Courts Administration Authority (CAA) computer processing environments. Those environments principally support the Oacis patient clinical management system, the Justice Information System and the Crimcase and FATE systems. The DHS environment utilises the Unix operating system while the CAA and the JTS managed systems reside respectively on the SYSC and SYSJ partitions of the EDS managed mainframe environments.

As part of the review of the JIS Audit also considered the management and control arrangements in place at agencies utilising the JIS. The agencies included SAPOL, the Attorney General's Department, and the Department for Correctional Services.

Audit also examined the general arrangements for business continuity planning.

Audit Findings and Observations

Computer Processing Environments

For the CAA, JTS and DHS managed environments the control environments were generally considered sound, although some potential exists to further improve specific security settings and control processes. The potential for improvement essentially relates to some system settings which could allow a small number of staff inappropriate access to the system.

The review also raised the critical issue of arrangements for continuity of operation of key government financial and operational systems. The review findings relating directly to the computer processing environments were communicated by Audit to DAIS/EDS and the three agencies concerned during the year.

DAIS and Agency Response *— DAIS and the agencies conveyed satisfactory action being taken in respect of the matters raised.*

DHS Response *— DHS has reviewed the matters raised and proposes that they be considered by the Information Management Technology & Communications Committee. This Committee was formed by the Statewide Hospitals Operations Group to develop and recommend strategies to achieve outcomes for information management systems, technology and communication infrastructure that support the clinical and administrative objectives of DHS.*

Business Resumption Planning

Previous reports to Parliament have made specific comment on the matter of Business Resumption Planning arrangements for certain government infrastructure services. As part of the review of the EDS IPC this important matter was considered relating to the computer processing environments covered in the review.

A draft 'Mainframe Disaster Recovery Plan' has been developed by EDS to cater for the various mainframe environments utilised by agencies within the South Australian Government. The plan, however, only caters for the restoration of the mainframe operating system and the database operating system software at the EDS data centre. With some exceptions it does not provide for the recovery of the various applications currently used by agencies. With regard to the wide area network, EDS is responsible for certain points that are installed at their data centre and a gateway device to the EDS

network located at a separate site in the Adelaide Metropolitan area. Individual agencies are responsible for establishing their own connections to this latter device.

With respect to this critical matter Audit recommended that the agreement between the government and EDS in relation to business resumption planning be progressed and formalised , that a risk assessment be carried out with some urgency to identify critical mainframe systems and the acceptable period for recovery. In this respect, it is essential for agencies to develop plans that address the components for the recovery for which they are responsible.

DAIS Response *— Agencies have previously defined their recovery requirements and priorities for mainframe systems and have recently been requested to update these requirements. DAIS understands that no agencies have made any changes to their recovery requirements or priorities. Agreed whole-of-government priorities for resumption of the various mainframe partitions have previously been agreed.*

In relation to midrange disaster recovery services, it is rightly noted, that this is the responsibility of the individual agencies to establish with EDS. At a whole-of-government level, EDS is obliged under the ITSSED contract to provide certain disaster recovery services for the mainframe business segment, but not necessarily for the other business segments of midrange, local area network, wide area network or workstation.

Critical mainframe applications have been identified along with the agreed priorities for recovery and estimated recovery times. These are outlined in a draft, working document 'South Australian Government Mainframe Disaster Recovery Strategic Plan' which has been jointly developed by DAIS and EDS. Supporting this, most agencies have tested the recovery of their individual mainframe partitions with EDS.

DAIS has previously issued a Change Request Proposal (CRP) to EDS for a whole-of-government mainframe disaster recovery test. DAIS has considered the response from EDS and has discussed the EDS and SAG responsibilities in relation to the costing provided. This matter had not reached a stage of finalisation at the time of preparation of this Report.

Audit will during 2003-04 follow up this important matter of business resumption planning.

CHAPTER 12 — AGENCY REVIEWS: DEPARTMENT FOR ADMINISTRATIVE AND INFORMATION SERVICES AND DEPARTMENT OF HUMAN SERVICES

CHRIS HRMS PAYROLL SYSTEMS — GOVERNMENT-WIDE

Background

The Minister for Human Services contracted with an external service bureau provider (bureau provider) for the provision of a Human Resource Management System (HRMS) and associated services for the Human Services portfolio. Similarly, the Department of Administrative and Information Services (DAIS), on behalf of a number of participating agencies of government, contracted for equivalent services with the same bureau provider.

The scope of the Complete Human Resource Information System (CHRIS) HRMS functionality includes; Payroll; Leave Management; Recruitment and Selection; and Training and Development. These strategically important projects involve the management of payroll and personnel functions for over 50 000 government employees in over 70 government agencies and health units.

Under the contracts with the bureau provider:

- Department of Human Services (DHS) is responsible for managing the contract and project implementation of the CHRIS HRMS system for the DHS Central Office and all health units.

- DAIS, acting as the lead agency for the Concept sector agencies, (now known as the Shared HRMS sector), is responsible for managing the contract and the project implementation of the CHRIS HRMS for participating agencies of government.

Audit Focus

During 2002, Audit has sought to determine the adequacy of controls over the bureau computer processing environments, managed by the private sector service provider.

In regard to that fundamental matter, DHS and DAIS in 2002 independently commissioned external IT security consultancy firms to collectively undertake five security reviews of the bureau facilities and IT infrastructure over a 12 month period. The key focus of the reviews was on the bureau's physical and infrastructure security, network, system and application security, disaster recovery arrangements, processes and procedures, and staff qualifications and experience.

These reviews have been completed and have been examined by Audit. At the time of preparation of this Report, DHS and DAIS were undertaking a joint consultancy for the provision of a Security Audit Update.

In August 2003, Audit conducted a separate review of key control aspects of the bureau provider computer processing environments. In addition, a review of the DHS Workforce Relations payroll/personnel processing and the DHS Central Support Unit activities was undertaken.

The review process conducted by Audit of the bureau provider computer processing environments and the DHS business units essentially encompassed the documentation and assessment of key control aspects of information systems operations; business continuity planning; IT security including logical security access authorisation and authentication practices; application systems implementation and maintenance; problem management, change management, user acceptance testing and software configuration release management practices; system software, network and hardware support.

In addition, Audit examined aspects of the relationship between DHS and the external bureau service provider, and, in particular, the conformance by both parties to the Bureau Services Agreement between the Minister for Human Services and the bureau provider.

At the time of preparation of this Report, a review of aspects of DAIS payroll/personnel processing and the Central Support Unit activities was in progress.

Audit Findings and Observations

Contracted Reviews

Essentially, the contracted security reviews revealed inadequate control exercised over the bureau service and IT infrastructure.

The IT security consultancy firms recommended regular security reviews while a new system such as this is undergoing frequent change. Audit considers this to be a prudent practice and that it is essential that the outcomes from security reviews are acted upon in a timely manner to ensure that whole-of-government systems and infrastructure are protected.

Audit's examination of the Bureau Services Agreements between the respective Departments and the bureau service provider revealed no direct reference within the Agreements to the bureau service provider complying with the latest government mandated security standards and procedures.

Important action items considered by Audit to be addressed by the respective Department were communicated to DHS in February 2003 and DAIS in March 2003. Audit sought advice from the Departments regarding their intent with respect to:

- finalisation of the outstanding issues from the contracted security reviews;
- completion of business continuity and disaster recovery testing;
- need for conduct of regular security reviews;
- inclusion of appropriate clauses in the Bureau Services Agreement with respect to the bureau service provider's compliance with specific government standards relating to Information Security Management.

Audit considered that the Departments should seek advice from the Crown Solicitor's Office as to the strategy and mechanisms for including appropriate clauses with respect to the bureau's compliance with specific government standards relating to Information Security Management.

DHS Response *— DHS responded in March 2003 advising the status of outstanding issues from the contracted security reviews. With respect to business continuity and disaster recovery planning, DHS stated that some testing was undertaken in October 2002. Testing of the plans was to be undertaken on a 12 monthly basis and plans for future testing in 2003 involved inclusion of DAIS operations for a whole-of-bureau contingency test. DHS advised that it intended to conduct further security reviews in collaboration with DAIS. DHS stated that it had written to the Crown Solicitor to include the relevant Government security standards in the Bureau Services Agreement.*

DAIS Response *— DAIS responded in March 2003 advising the status of outstanding issues from the contracted security reviews. With regard to business continuity, DAIS advised that a generic Business Continuity Plan had been approved with agencies agreeing to use it as the basis for developing their individual agency Business Continuity Plans. DAIS advised that a test of the disaster recovery arrangements was carried out and documented in January 2003. Further testing of disaster recovery would be undertaken following the completion of the Shared HRMS implementation. Further security reviews were scheduled and appropriate information security management clauses in the Bureau Services Agreement relating to compliance with government standards were included in proposed contract variations.*

Audit Review

Audit's review in August 2003 of the bureau service provider computer processing environment and the DHS business units, found that with respect to matters of security and control:

- security over access to the Electronic Funds Transfer file at DHS Workforce Relations was not secure;

- DHS documented Disaster Recovery Plans were not up-to-date or tested.

Audit communicated these issues to DHS in writing in October 2003.

DHS Response *— DHS responded in November 2003 advising that it had restricted access to the Electronic Funds Transfer file to specific privileged users. Regarding Disaster Recovery Planning, system wide testing was still required and a test plan had been provided to the bureau provider for review and finalisation by November 2003. DHS Central Support Unit Disaster Recovery Plan was being reviewed. Outstanding health unit Disaster Recovery Plans were escalated to various governance committees.*

CHAPTER 13 — AGENCY REVIEW: DEPARTMENT OF EDUCATION AND CHILDREN'S SERVICES

EDUCATION DEPARTMENT SCHOOL ADMINISTRATIVE SYSTEM

The Department of Education and Children's Services (DECS) Education Department School Administrative System (EDSAS) is used to manage school staff and student records, financials, and profiling capabilities within individual schools and also provides a reporting capability for the DECS Head Office. Management of the system with respect to its development and overall support is coordinated through DECS Head Office.

The system is used throughout approximately 600 schools and contributes substantially to the achievement of educational outcomes within the South Australian education sector.

Audit Focus

Audit's review focused on a selected sample of 10 schools and the DECS Head Office operations.

In relation to schools, areas covered included the management of EDSAS and its supporting infrastructure, operation of the finance module within EDSAS, and maintenance of school census information. The 10 schools were selected to form a representative sample from the total school population. Schools selected were the Kilburn Primary; Mansfield Park Primary; Marion Primary; Croydon High; Underdale High; Adelaide High; Aberfoyle Hub High; Modbury High; Norwood/Morialta High; and Aberfoyle Primary schools.

The DECS Head Office areas of coverage included strategic planning, training and support, policies and procedures, change management, and release management processes.

Audit Findings and Observations — Schools

In late 2002 Audit communicated its findings and recommendations to each of the schools reviewed. Responses from all schools were received by early 2003. The following summarises Audit's key findings and observations.

Management of EDSAS and Supporting Infrastructure

In relation to management and security of EDSAS there were a number of important control weaknesses that needed to be addressed. Some of the more important weaknesses noted in respect of some schools were:

- Inadequate user access arrangements to the EDSAS system application and school network.
- Inappropriate storage of backup media, incomplete backup and lack of testing of backups.
- Lack of appropriate environmental controls such as air conditioning and fire extinguishing equipment.

- Inadequate physical security of the EDSAS computing infrastructure.
- Lack of virus protection software.
- No formal documented disaster recovery and business continuity procedures.
- No uninterruptible power supply for the EDSAS computing infrastructure.

Finance Module of EDSAS

Financial controls were generally satisfactory. An important matter identified was the level of segregation of duties in schools, which was impacted by the available school resources. Inappropriate segregation of duties presents a risk of accidental financial errors and a risk of fraud resulting in financial loss.

Audit recommended certain controls that could be implemented at both large and small schools to address the segregation of duties matter.

School Census Information

Audit found no significant concerns in relation to the maintenance of student records, and the procedures related to school census report validation, acceptance and auditing were considered satisfactory.

Audit Findings and Observations — Head Office

In March 2003, Audit formally communicated to DECS in a comprehensive report, the findings and recommendations of the review and received a response in May 2003. Considering the strategic importance of this system in the provision of education outcomes within the South Australian public education sector, Audit undertook a follow up review in October 2003 and received an updated detailed response from DECS in November 2003. The responses were the subject of discussion between Audit and senior management of DECS.

Strategic Planning

Audit in discussion with the Department, recognised the importance to DECS of maintaining an up-to-date overall IT strategic plan for new developments and systems, including EDSAS. Such a plan evidences a diligent planning basis and serves to underpin IT investment decisions and approvals.

Audit recommended, amongst other things, that identified development and improvement issues with the EDSAS system be considered in the context of the proposed documentation of an updated Department IT strategic plan covering all DECS systems.

Training and Support

There was a need for improvement in relation to training which requires DECS and the schools to revisit the delivery and funding approach to training. The need for improved training was evidenced during the review of schools where a number of issues and inconsistent practices were identified.

Audit recommended that DECS establish a systematic training program that should provide a guideline of minimum basic skills required to perform particular roles or functions. Further, it was recommended that DECS in conjunction with the schools, determine an appropriate funding model for the establishment and ongoing training of the systematic training program.

Policies and Procedures

Whilst a wide range of documentation exists, the formal EDSAS procedural manuals do not specifically address some fundamental key procedures for the management and security of EDSAS. Certain documentation exists which address these items to varying degrees. In many cases school staff were not aware of current documented procedures.

Audit recommended that DECS revise and consolidate its existing documentation and maintain a central register of documentation. That register would include both documentation related to head office activities and documentation distributed to schools. Further, a process should be established to ensure that school based staff are made aware of all current procedures and guidelines.

Change Management

Important areas of control of new versions of the EDSAS system were identified as requiring improvement with respect to formal sign offs relating to upgrades and new releases of the system. Schools staff advised a high number of problems within EDSAS which would require new versions to be produced.

Audit recommended that all changes to EDSAS, be signed off by a designated data/system owner prior to release, and that the processes for submitting requests for change be simplified.

DECS Response *— DECS formally responded to the two management letters from Audit, and in its most recent response of November 2003, gave an update to the earlier response and advised of progress and status of actions proposed and taken in relation to Audit's recommendations. DECS essentially advised that:*

Planning — A project to document an up-to-date IT strategic plan was underway and scheduled for completion in January 2004.

Training and Support — A Training and Development Working Party has been established including representatives from Principals, Finance Officers, EDSAS Managers and Business Managers to investigate the training options. DECS has also indicated it will investigate existing funding and possible future funding models, involving schools meeting their training and development responsibilities. Other initiatives include:

- *A revised EDSAS management framework is being established to ensure appropriate process and consultation or advice as required. That framework consists of an EDSAS Management Group and Reference Groups for the three functional areas of administration, finance and curriculum.*

- *An EDSAS Reference Group structure to support stakeholder input and prioritisation of EDSAS issues was to be established in late 2003.*

- *A new Knowledge Analyst position has been created which is responsible for the DECS Knowledge Management function. A key role is to identify relevant knowledge and information and establish options for improved dissemination of that knowledge and information.*

- *The EDSAS Support Team has been incorporated with the Application Services Unit with the view to being subject to a more robust framework of procedures, standards and support services to improve the integrity and security of EDSAS.*

- *The Department is implementing a new district structure supported by central coordinated services.*

IT Security and Control — DECS is developing an IT Security Review and Management Review pack which will be in place by early 2004. The aim of this document is to provide guidance to schools in respect of matters of security to be considered and addressed.

In summary, the review identified many opportunities for improvements that Audit considers should be addressed by DECS to ensure the efficient and effective use of EDSAS and the maintenance of adequate standards of security and integrity regarding its operation. Areas of training and policy and procedures are significant matters for the Department as they have an influence on the efficiency and effectiveness of education administration and financial management of schools.

Regarding the matters raised by Audit, DECS has initiated actions aimed at achieving improvement. These include revisiting its planning for EDSAS in conjunction with overall strategic planning for the Department, revising existing management structures, initiating a training and development working party, investigating future funding models, improving controls over new software versions, and taking action to address EDSAS security weaknesses.

The detailed response identified actions in progress or to be completed by certain timeframes. Those timeframes in some instances provide for completion during the 2004 school year. The Department's response is reasonable in recognition of the nature of the matters being addressed and outcomes to be achieved.

Audit will review the progress and completion of these matters in 2004.

CHAPTER 14 — AGENCY REVIEW: DEPARTMENT FOR ENVIRONMENT AND HERITAGE

COMPUTER PROCESSING ENVIRONMENTS

Audit reviewed certain key computer processing environments which support financial information and operational systems within the Department for Environment and Heritage (DEH). The review process encompassed the documentation and assessment of organisational management, computer processing environments, systems and associated internal controls for the following areas:

Strategic Policy and Planning — high level strategic policy and planning for the Department's business operations, including organisation, resource strategy and planning, business continuity planning, security policy and procedures and the use of communications networks and Internet/intranets; and

Computer Processing Environments (Mid Range, LAN, Stand Alone) — information systems operation, relationships with outsourced vendors, logical and physical security, application systems and database implementation and maintenance, and network and systems software support.

The high level assessment identified important areas of a broad level planning, policy and procedural nature and security control arrangements that were considered in need of management attention to effect required improvements were communicated to DEH in October 2002.

Audit Findings and Observations

Some of the more salient management and control matters requiring improvement were:

- revisiting the DEH IT Strategic Planning to cover the period 2002 and beyond and ensuring appropriate Committee arrangements are enabled for the effective monitoring of IT Strategic Planned developments;
- updating and reissuing its Business Continuity Plan and having measures in place to ensure that the plan is reviewed, updated and tested on a regular basis;
- reviewing and updating Service Level Agreements with external vendors relating to ownership and support of DEH infrastructure;
- approving and conveying to staff the updated DEH security policy and procedures;
- improving password management and control practices and procedures.

DEH Response *— DEH advised in January 2003 that the Department had recently clarified its role and functions with the establishment of the Environment and Conservation portfolio. Consequently, the IT Strategic Plan would be influenced by changes within the portfolio and was scheduled to be completed in mid 2003. In addition, Committee arrangements would be reviewed as a result of organisation change activities.*

DEH further advised that business continuity activities would be undertaken on an opportunistic basis and scheduled with other priority projects. Updating of Service Level Agreements had been included in the role of the recently established IT Contracts Manager. Security policies have been approved and communicated to staff via the DEH intranet. Password management and control practices and procedures have been corrected.

CHAPTER 15 — AGENCY REVIEW: HEALTH UNITS

CERTAIN COMPUTER PROCESSING ENVIRONMENTS

Health units are major service providers within the Department of Human Services (DHS) portfolio and are significant users of Information Technology critical to the health unit business and service delivery outcomes.

Three major health units in the portfolio are the Flinders Medical Centre (FMC), North Western Adelaide Health Service (NWAHS) and the Royal Adelaide Hospital (RAH).

Audit Focus

Audit assessed certain key computer processing environments which support financial information and operational systems within the FMC, NWAHS and RAH health units. The review addressed aspects of organisational management, systems and associated internal controls for the following areas:

- Strategic policy and planning
- Business continuity planning
- Security policy and procedures
- Information systems operation
- Aspects of database maintenance, and network and systems software support.

Audit Findings and Observations

The critical areas of planning, policy and procedures, and security and control arrangements were considered in need of management attention to achieve a satisfactory control environment. These were communicated to each of the health units between July and August 2002.

With respect to strategic and management matters, two of the health units reviewed (FMC and NWAHS) needed to revise their IT Strategic Plans and have the plans formally endorsed by management. Audit noted that the reinstatement of formal Information Systems governance arrangements for two health units (NWAHS and RAH) needed to be considered.

Some of the more salient management and control matters requiring improvement which were consistent across the three health units reviewed are summarised as follows:

- Key aspects of Business Continuity planning, procedures, implementation and testing and disaster recovery planning for all sites were not in place.

- Security configuration within certain critical applications at health unit sites needs to be reviewed and improved.

Recommendations were made to two health units (FMC and RAH) to formalise documentation with respect to supporting the health unit's systems development and maintenance methodology. Further, unrestricted access to production environments by systems support and/or analyst programmer personnel needed to be addressed at two health units (FMC and NWAHS).

A recurring issue for health units, reinforced by the reviews undertaken within the FMC, NWAHS and RAH health units, is that of formal procedures and testing to ensure business continuity and disaster recovery. Health units in general have not revisited the risk assessment in relation to their systems and facilities since the major thrust undertaken as a result of the Year 2000 millennium concern.

Health Unit Responses — *All of the above health units responded in September 2002.*

FMC advised that it intended to undertake and internal review and develop an IT Strategic Plan to complement the DHS 10 year IT Strategic Plan once the DHS plan is finalised. Regarding Business Continuity planning, FMC stated that review and testing of key elements of the plan would be completed by the end of the 2002-2003 financial year. Security configuration for a certain software application was to be upgraded by December 2002. Completion of documentation of the IT systems development and maintenance methodology would be completed in the first quarter of 2003.

In its response, NWAHS stated that an Information Services Committee had been reinstated and would be fully operational by the end of September 2002. NWAHS advised that development of an Information Technology and Telecommunications strategic plan depended upon the finalisation of the DHS 10 year IT Strategic Plan, the government direction for the two campus' of the NWAHS and the IT&T restructure. Business contingency plans were in the process of updating and would be completed by the end of November 2002. Aspects of security policies, procedures and application configuration would be addressed by December 2002.

RAH advised that the reinstatement of an IT Forum was being planned. The response indicated that a number of projects were underway that addressed some of the issues raised by Audit. In addition, integration of the Prison Health Service and the Glenside Mental health Service with the RAH North Terrace facilities had commenced. An external consultant had been engaged to develop, review and exercise specific Disaster Recovery Planning by March 2003. IT Policy documentation was being updated and expanded.

Audit recently commenced follow up reviews at the three health units.

The NWAHS and RAH had responded at the time of preparation of this Report.

The NWAHS November 2003 response advised that the Information Services Committee will be reconvened. It would be instrumental in reviewing the IT&T Strategic Plan 2002-2004 and making recommendations to Executive. With regard to business continuity, Audit was advised that a TQEH risk register is being developed as is the development of a Business Continuity Plan. Security policies and procedures would be forwarded to the Operations Executive Group for consultation and endorsement. Aspects of security configurations for certain applications were being addressed.

The RAH November 2003 response advised that a draft Disaster Recovery Plan for the Patient Management System has been developed and other applications would be assessed to develop Disaster Recovery Plans for these systems. Assessment of the Oacis system as an alternative to the disaster recovery for the Patient Management System has had commenced with an anticipated outcome in early 2004. The Glenside campus contingency plan was to be developed as a component of an overall RAH plan. The RAH IT Policy documentation was being updated. Security event and Internet user access authentication and monitoring was now operational.

Follow up with FMC is still in progress.

CHAPTER 16 — AGENCY REVIEW: INDEPENDENT GAMING CORPORATION LTD

GAMING MACHINE MONITORING SYSTEM

The Independent Gaming Corporation Ltd. (IGC Ltd) operates a central computerised monitoring system which monitors and records the activities of over 15 000 individual gaming machines located in approximately 600 venues in the State. Operation of the gaming machines contributes millions of dollars to the State's revenue base, and is subject to regular Parliamentary and media debate.

The Liquor and Gambling Commissioner, in granting the Gaming Machine Monitoring License, established stringent conditions of acceptance for the operations of the computerised monitoring system. IGC Ltd, in discharging its responsibilities in respect to monitoring of gaming machine operations in licensed venues has, with the Treasurer's approval, set a charge on licensed gaming machine operators to provide for the ongoing cost recovery of its operations.

Monitoring system maintenance contracts exist with various companies. Under the provisions of the *Gaming Machines Act 1992* (Gaming Machines Monitoring Licence Conditions), IGC Ltd may not alter or maintain the monitoring system hardware or software. Only third parties approved by the State Supply Board (the holder of the Gaming Machine Supplier's and Service Licences) may do so. As such, IGC Ltd. has a number of maintenance contracts with approved third parties for the maintenance of monitoring machine hardware and software.

Audit Focus

In the last two years, Audit has undertaken focused reviews of certain technical aspects of the Gaming Machine Monitoring System (GMMS) and Internet web site facility. The reviews included consideration of the:

- policy and procedural documentation in relation to the GMMS and Internet web site facility;
- nature and extent and outcomes of Internal Audit activity;
- performance of review work associated with the system database administration and security, backup and recovery and change management processes.

It is important to note that the environment that IGC Ltd operates in, notably with a technically advanced GMMS and a small number of staff, places increased emphasis on a number of matters. These include the need for comprehensive policy and procedural documentation, training of staff, and regular monitoring of key activities, particularly with respect to the GMMS but also the Internet web site facility.

Audit Findings and Observations

The audit reviews have confirmed IGC Ltd, through its Board Audit Committee and Management, has exercised diligence with respect to the overview of security and control practices in operation of the GMMS and Internet web site facility.

The reviews did make recommendations to further improve the overall security arrangements regarding the GMMS and Internet web site facility. Audit's recommendations addressed some aspects of:

- documented security procedures;
- audit logging and monitoring of critical GMMS information;
- direction and scope of IGC Ltd Internal Audit strategy.

IGC Ltd Response *— Responses received from IGC Ltd in respect of the matters raised over the past two years demonstrate a positive approach to all matters raised.*

CHAPTER 17 — AGENCY REVIEW: DEPARTMENT OF PRIMARY INDUSTRIES AND RESOURCES

COMPUTER PROCESSING ENVIRONMENTS

Audit reviewed certain key computer processing environments which support financial information and operational systems within the Department of Primary Industries and Resources (PIRSA). The review process encompassed the documentation and assessment of organisational management, computer processing environments, systems and associated internal controls for the following areas:

Strategic Policy and Planning — high level strategic policy and planning for the Department's business operations, including organisation, resource strategy and planning, business continuity planning, security policy and procedures and the use of communications networks and Internet/intranets; and

Computer Processing Environments — information systems operation, relationships with outsourced vendors, logical and physical security, application systems and database implementation and maintenance, and network and systems software support.

Audit Findings and Observations

A number of important areas were identified that related to planning, policy and procedures, and security and control arrangements that were considered in need of management attention to achieve a satisfactory control environment and these were communicated to PIRSA in August 2002.

Some of the more salient management and control matters requiring improvement were:

- key aspects of Business Continuity planning, procedures, implementation and testing and disaster recovery planning were not in place;
- security configuration within certain critical applications at PIRSA sites needs to be reviewed and improved;
- formal documentation supporting certain system development and maintenance methodology had not been prepared and put in place;
- analyst programmer unrestricted access to the production environment needs to be reviewed.

PIRSA Response *— PIRSA advised in September 2002 that the Department had undertaken several recent initiatives which addressed most of the findings and recommendations identified in the review. This included conducting a formal IT security review of computer processing environments, upgrading to an approved commercial project methodology for application development and redevelopment, and establishing the role of IT Configuration Manager. Business continuity was planned to be addressed in late 2003.*

Audit conducted a follow up review of the above findings and response in August 2003.

PIRSA Response *— PIRSA's formal response in August 2003 outlined action being progressed and envisaged completion timeframes with respect to the matters raised. Key matters raised are planned to be significantly progressed or finalised by the end of 2003.*

Audit will during 2003-04 follow up these matters.

CHAPTER 18 — AGENCY REVIEW: SENIOR SECONDARY ASSESSMENT BOARD OF SOUTH AUSTRALIA

RESULTS PROCESSING SYSTEM

The operations of the Senior Secondary Assessment Board of South Australia (SSABSA) are an important component in the provision of education outcomes within the state of South Australia. SSABSA annually provides the academic results for over 22 000 students throughout the State and in the Northern Territory. These results provide the basis for University entrance offers made to those students in the following year.

SSABSA has developed its Results Processing System (RPS) to process student achievement data and results information during the critical end of academic year results processing period. SSABSA has for many years attained considerable success through the operation of the RPS.

The RPS is a system that has its own unique operating and design characteristics, being an internally developed system, with significant effort expended in data management and data purification. Additionally, certain operations require a high level of managerial judgment.

Audit Focus

Audit's review was directed towards ascertaining whether the security and control mechanisms relating to the RPS were appropriate including consideration of potential future developments to the system.

The review entailed the assessment of the specific matters of strategic IT management; contract administration; operations and communications network management; RPS Security, System Development and Support; Business Continuity Planning; and the Web site facility.

Audit Findings and Observations

Audit found the RPS provides an adequate level of functionality and control over operations. More specifically, Audit formed the view that important areas of operations management and system development and support are appropriately controlled, notably the areas of data management, configuration management, and scheduling.

Notwithstanding, there were certain matters that Audit considered as important to the overall ongoing management of security and control arrangements. These mainly involved a focus on the strategic direction of the RPS, improving the level of documentation of the system's design and operation, and the consideration of more formal business risk management arrangements.

At the strategic level, it was considered appropriate for SSABSA to incorporate into its strategic planning process, aspects relating to the development of the RPS and related applications.

Improvements in documentation involved the need to update the strategic plan, design and operational documentation, contingency planning and user documentation.

A need to implement a formal business risk management regime was also identified given the nature of the agency and its operations.

These matters were communicated in writing to SSABSA in September 2002.

SSABSA Response *— SSABSA advised in November 2002 that it will consider each of Audit's recommendations in detail and develop an implementation plan to address each of the issues raised. In addition, with regard to matters raised in relation to Business Risk Management, SSABSA have commenced a comprehensive risk assessment of each of its Branches with a view to developing a formal risk management program for the whole organisation.*

Given the nature of the core business and the timing of the review response (a time when the peak load is on the RPS) SSABSA intends that these matters will be addressed in 2003.

Audit will follow up the status of matters raised after the 2003 results processing process.

CHAPTER 19 — AGENCY REVIEW: SOUTH AUSTRALIAN POLICE DEPARTMENT

CAPTURE ADJUDICATION AND REPORTING SYSTEM

The South Australian Police Department (SAPOL), through its Expiation Notice Branch (ENB) within Business Service is responsible for the administration of Department expiation notices. A major source of expiation notices is a result of the operation of red light and speed cameras. During 2001-02, in excess of 300 000 notices were issued with a value of more than $49 million.

The computer system used to support these activities is the Capture Adjudication and Reporting System (CARS). CARS is an integrated software and hardware solution system that has been developed under arrangements with an external contractor to provide computerised film scanning, adjudication, archiving, document management and reporting services and to incorporate technologies such as digital film processing and optical character recognition.

Audit Focus

Audit's review considered key controls for information security; system operations; systems implementation and maintenance; business continuity; and control aspects of database support, communications networks, systems software and hardware support.

Audit Findings and Observations

A number of important areas were identified that needed management attention to effect significant control improvements and these were communicated in writing to the Department in October 2002.

The review revealed a need for:

- improvement principally in certain technical control settings and processes which represent a potential risk for local and network access to the system;
- additional configuration and security enhancements of CARS and establishment of service level agreements to satisfy Police Department Infrastructure, Desktop, Applications and EDS support groups;
- inclusion of the CARS system in the SA Police Department business continuity plan and testing of the disaster recovery procedures;
- separation of ongoing development, maintenance, testing, quality assurance and production functions on the CARS computer to ensure appropriate standards of integrity of data;
- establishment of a documented change management process to support the CARS computer or supporting workstations;
- an operational needs analysis of CARS to ensure all Police Department business and operational standards are incorporated within the supporting infrastructure.

Police Department Response *— A formal response was provided in November 2002. The response stated that representatives from the Department and the external contractor had corrected operating system and database security vulnerabilities.*

A responsibility matrix between Information Systems and Technology (IS&T), ENB, EDS and the external contractor had been developed. Issues such as backup and recovery arrangements, server and system monitoring were to be the responsibility of IS&T and EDS after the transfer of responsibility of the server from ENB.

An additional server was to be provided for extensive changes to the CARS system which would then be used to test disaster recovery and to separate development and testing from the operational server. In addition, the Department ENB established processes with respect to change control.

In September 2003, Audit conducted a follow up review on the above recommendations and response and communicated with the Department in writing in October 2003.

The Department responded in November 2003 confirming advice to Audit that a draft responsibility matrix with EDS had been broadly agreed. Cabinet had approved a submission in April 2003 for $1.4 million for enhancements to the CARS system to satisfy government Road Safety Reform initiatives and the initiatives would be operational by December 2003. A business recovery test had been conducted and Disaster Recovery Plans had been completed.

In summary, the development and implementation of the CARS system was undertaken with the joint cooperation of SAPOL and an external contractor. The Audit review, identified many opportunities for improvement to the system. The Department discussed the outcomes with Audit and related with the external contractor and proactively instituted a plan of action to address the issues identified.

Audit will review the progress of these matters in 2004.

CHAPTER 20 — AGENCY REVIEW: UNIVERSITY OF SOUTH AUSTRALIA

REMOTE ACCESS FACILITY

The University of South Australia has a remote access facility that allows certain staff and certain post-graduate research students to access the University's network and its associated resources through an external dial up connection. The remote access facility itself consists of a dedicated computer through which dial-in modems and associated network authentication computers are connected.

One consideration in undertaking this review was a general concern regarding the wide level of access provided to the internal University network available through the remote access facility.

Audit Focus

Audit reviewed the remote access facility at the University with specific reference to the provision of access via this facility to the Finance and Human Resources Systems. The objectives of the review were to ascertain the extent of the exposure of the Finance and Human Resource systems to the external access facility and the Internet and to identify improvements to the control environment if appropriate.

Audit Findings and Observations

While Audit did not identify any instances of inappropriate access, a number of important matters were identified that were considered in need of management attention to affect required control improvement.

Among the more relevant matters conveyed in writing to the University in August 2002 were the:

- University progress the implementation of its current software upgrade plan so that the extra functionality made available for preventing internal access to selected computers from the remote access facility can be implemented and to rationalise the administration of network based resources;

- University develop a suitable planning framework for addressing security management issues related to the overall network as it currently exists to take account of deficiencies in its architecture and facilities and amends this planning framework to consider changes to the infrastructure as they occur. This planning framework will form the basis for implementing changes to infrastructure and operating procedures to more effectively manage the overall environment from both a management and security point of view;

- various systems administrators, including those managing the Human Resource Management application and related network infrastructure services, perform log analysis with a view to determine any trends in access that may indicate unauthorised activity. It was recommended that the University investigate improvements to the logging of security related events for the Finance system and improvements to reporting for the remote access facility computer;

- University implement procedures to ensure that staff terminations and relocations are advised in a timely manner to relevant areas requiring this information within the University;

- University provides appropriate training to a suitable staff member to become a backup administrator for the Finance system.

University Response *— The University advised in September 2002, that various aspects of the report would be actioned. These included more formalised arrangements for assessing risk to the networks, more formalised procedures for analysis of available logs, investigation of improvements to the logging of security related events for the Finance system and reporting for the remote access computer.*

Audit sought an update regarding the above issues in September 2003 and at the time of preparation of this Report, Audit was in the process of following up this matter.

PART 4 — IT LEGAL CONSIDERATIONS IN ELECTRONIC GOVERNMENT

PART 4 — IT LEGAL CONSIDERATIONS IN ELECTRONIC GOVERNMENT

TABLE OF CONTENTS

PART 4 — IT LEGAL CONSIDERATIONS IN ELECTRONIC GOVERNMENT

TABLE OF CONTENTS

CHAPTER 21 — REVIEW BACKGROUND AND KEY FINDINGS AND COMMENTS

BACKGROUND

Introduction

Audit Reports to Parliament for the last few years have provided comment on certain legal and management aspects of e-government operations. This has been done through the review of a number of e-commerce reviews in selected agencies, mainly involving contracts with the private sector.

This Part presents the findings of further work completed by Audit during 2002 and 2003. During this period Audit has reviewed the legislative framework for electronic government, and has examined some major electronic commerce and web site facility developments to determine the adequacy of the control environment associated with these matters.

Audit Mandate

The Audit review process was conducted pursuant to section 36 of the *Public Finance and Audit Act 1987.*

AUDIT APPROACH AND COVERAGE

During 2002 and 2003 Audit examined the legislative framework for electronic government which was the subject of comment in my 2001 Report. The focus of work in this area was mainly directed at developments with respect to the *Electronic Transactions Act 2000* (SA) and the matter of privacy.

Audit also selected a range of agency initiatives for review. These initiatives involved matters concerning government Internet web site entry points for services, the keeping of medical records, and electronic financial transaction processing.

Audit's reviews have focused on matters of a legal and contract nature and examine aspects of risk management arrangements in the selected agencies. The reviews also addressed agency web site facilities for compliance with government requirements and better practice management.

The sensitive area of medical information has been addressed with the review of the 'Oacis' programme of the Department of Human Services. This programme will be fully implemented in 2005.

Other agencies and projects selected covered electronic commerce facilities, web sites for financial transaction processing of motor vehicles and drivers licences, and the electronic lodgement of court documents. The revenue raising area of taxation is addressed with a review of payroll tax and a look at the RevNet project in the Department of Treasury and Finance.

A follow up review of certain matters relating to the 'SA Central' web site was also undertaken.

KEY AUDIT OBSERVATIONS

My last Report on Electronic Government described and considered the major forms of legal regulation potentially applicable to e-commerce.[11] It is not proposed to revisit that commentary, other than to note one significant development since it was published, ie the proclamation of the *Electronic Transactions Act 2000* (SA). Certain key observations and comments are also made with respect to the important matter of privacy and important issues arising from the various reviews of agency electronic commerce developments.

Electronic Transactions Act 2000 (SA)

As explained in my last Report on this matter, the Act provides that, as a general rule, any requirement under South Australian law that information be given, recorded, or verified in writing may be met or carried out electronically, subject to appropriate safeguards being observed for the protection and integrity of the data.[12]

The Act was proclaimed with effect from 1 November 2002. As provided for under the Act, regulations have also been introduced that exempt certain 'writing requirements' from the operation of some of its provisions.[13]

The most significant of these requirements relate to:

- dealings with an interest in land;
- the witnessing or verification of a document by someone other than the document's author;
- delivery of a document by 'personal service' only;
- consumer credit transactions.

As highlighted in some of the agency developments reviewed, notably that relating to Transport SA's e-commerce system for motor vehicle registrations and driver licensing, agencies involved in electronic transactions will need to be aware of the circumstances in which the 2000 Act will and will not apply.

It is not merely the exclusionary regulations that are important in this context, but the limitations that are inherent in the Act itself. In particular, the mere fact that a requirement that information be supplied or recorded in writing may, under the Act, be satisfied by an electronic communication does not mean that a particular form of communication will in fact comply with the Act's requirements in relation to data integrity.

Any agency that is establishing an e-commerce system in the context of a regulatory framework that includes 'writing' requirements needs to satisfy itself that the forms of

---

11 Report of the Auditor-General for the year ended 30 June 2001, Part A, pp 160-178.

12 Report of the Auditor-General for the year ended 30 June 2001, Part A, pp 162-163. See also *Electronic Transactions Act 1999* (Cth), which makes provision to the same effect in relation to requirements under federal legislation.

13 *Electronic Transactions Regulations 2002* (SA)

communication and/or record-keeping envisaged under the new system will actually fulfil those requirements, if necessary on the basis of the 2000 Act.

Privacy

Although the situation has not changed, it is to be noted that unlike some other States such as New South Wales and Victoria,[14] South Australia does not have privacy legislation that covers the State public sector.

As explained in my 2001 Report,[15] while the *Privacy Act 1988* (Cth) now applies to federal government agencies and a range of businesses in the private sector, South Australian Government agencies are covered only by an administrative direction to observe certain Information Privacy Principles (IPPs).[16] These are based on, though not identical to, the IPPs that apply to Commonwealth agencies under the 1988 Act, and are less extensive than the National Privacy Principles (NPPs) that the Commonwealth Act imposes on private sector organisations.

The problems that can potentially arise as a result of the differences between these various sets of principles are highlighted in the 'Oacis' review in this Report.

The non-statutory basis for privacy protection in South Australia means that South Australians may have no enforceable rights to access and/or control the use of information about them held by State government agencies. This is a matter that should arguably be dealt with by legislation which at the very least requires such agencies to abide by the IPPs applicable to their federal counterparts under the 1988 Act and provides a mechanism for individuals to lodge complaints where such principles are breached.

Agency Electronic Commerce Developments

Audit found that there are certain risks evident in agency management of electronic government transactions and the management and control of web site facilities and information. Some of these risks arise from inadequacies in the existing legislative framework. These matters include:

- A need for revision of certain State legislation, notwithstanding the introduction of the *Electronic Transactions Act 2000* (SA), requiring written forms of communication and/or record keeping with respect to electronic commerce systems being used by some government agencies. A particular example is the *Stamp Duties Act 1923* (SA).

- Inadequacies in agencies' risk management arrangements when outsourcing electronic initiatives with the private sector.

- The risk of inaccurate data entry and breaches by third parties.

- Intellectual Property rights not in all cases, being properly documented.

---

14 See *Privacy and Personal Information Protection Act 1998* (NSW); *Information Privacy Act 2000* (Vic).

15 Report of the Auditor-General for the year ended 30 June 2001, Part A, pp 169-171.

16 South Australian Government Administrative Instruction No 1 of 1989, located at www.archives.sa.gov.au/services/public/privacy_index.html

- Standard web site disclaimers being inadequate for some key agencies.

INDIVIDUAL AGENCY REVIEWS

Specific agencies and initiatives reviewed and commented on in the following Chapters of this Part of this Report are:

Department for Administrative and Information Services	SA Central Web Site. Service SA Web Site.
Courts Administration Authority	Magistrate Court Electronic Lodgement Service Courts Administration Authority Web Site
Department of Human Services	Oacis Programme. HealthySA Web Site.
Department of Transport and Urban Planning — Transport SA	Registration and Licensing Initiative.
Department of Treasury and Finance — RevenueSA	Payroll Tax Collections RevenueSA Web Site RevNet

Findings arising from the agency reviews have been formally communicated to, and discussed with the agencies and, where appropriate, with DAIS, and responses received.

OVERVIEW OF ISSUES ARISING FROM AGENCY REVIEWS

By way of an overview, the following is a summary of the general issues that are discussed in greater detail in the following Chapters in this Part.

Legislation — With respect to the need for revision of certain State legislation requiring written forms of communication and/or record keeping, changes relating to some key legislation have been initiated through Cabinet approval processes and were being progressed at the time of preparation of this Report.

The *Stamp Duties Act 1923* was identified as one principal Act requiring review in this context.

Privacy — As mentioned above, South Australia does not have privacy legislation that covers the State public sector.

Regarding the matter of privacy, in September 2003, DAIS advised Audit that it would convene a meeting of agency representatives, including officers from a corporate policy background and ICT specialists, in preparing a proposal for consideration by the ICT Strategies and Standards Steering Committee and the MPICC prior to the making of a submission to Cabinet.

Web Site Facilities - Disclaimers — The SA Central web site contains a legal disclaimer. This disclaimer has often been used as a basis for other government web sites.

Use by government agencies of disclaimers on agency web sites was generally appropriate. However, the SA Central disclaimer should, in my opinion, represent the

minimum disclaimer used by government agencies. This general disclaimer should be supplemented as necessary to accommodate the situation applicable in the specific circumstances of each individual agency.

Intellectual Property — Intellectual Property (IP) rights were not in all cases properly documented.

IP rights should be addressed in formal agreements. As a risk minimisation measure agencies should ensure that the Government owns the IP rights to any content published. Where this is not the case, appropriate acknowledgements should be made.

General — It is relevant to note, in a general context, that the agency developments reviewed herein are not being adequately coordinated and monitored, and are at varying levels of development, implementation, and sophistication. This is particularly so as regards the electronic procurement area of government, when compared with some interstate developments.

As mentioned in Part 1 of this Report the matter of the importance of high level government overview of these important electronic commerce developments has been communicated to DAIS.

CHAPTER 22 — AGENCY REVIEW: DEPARTMENT FOR ADMINISTRATIVE AND INFORMATION SERVICES

SA CENTRAL WEB SITE

Background

'SA Central' is the Department for Administrative and Information Services (DAIS) managed web site. This web site supplies information and links to other web sites.[17] It is intended to be the first and main point of contact for anyone seeking information regarding State Government activities and a variety of government and private services that may be accessed through the internet.

Audit Follow Up Review

In 2003, Audit undertook a follow up review of certain matters relating to the SA Central web site. One matter of interest arising from the review that has general applicability across government is that of the use by government agencies of the 'disclaimer' used on the SA Central web site as being adequate for all governmental purposes. For the reasons discussed hereunder that is not necessarily a prudent assumption to make.

Disclaimer Use

The SA Central disclaimer is in wide use by a variety of entities within the South Australian Government. The disclaimer is broadly drafted, and refers to the 'Government of South Australia' rather than a specific department or other government entity. It should be noted by all government entities, whether a department, statutory authority or other entity, that this disclaimer should represent the minimum disclaimer used by that government entity.

Each entity should review the disclaimer carefully and add to it as necessary to satisfy the particular circumstances that are relevant for the purposes of that entity.

Careful consideration should also be given to the appropriateness of merely 'linking' to the disclaimer rather than incorporating it into the individual entity web site.

Linking serves the purpose of requiring minimal effort to ensure any updates are included into the disclaimer. If changes are made to the linked site, then the changes are automatically caught through the link. But linking also opens the possibility of the disclaimer being unavailable for some reason or the wording of the disclaimer reached by a link may be such that it is not clear whether the disclaimer refers to the site on which the disclaimer resides or the site to which the disclaimer is linked. This last issue is one which has arisen in the context of this review.

It is commented on in more detail in relation to other web sites.

SERVICE SA WEB SITE

Background

The South Australian Government through the Department for Administrative and Information Services (DAIS) provides a web site[18] containing information concerning

---

17 www.sacentral.sa.gov.au

18 www.service.sa.gov.au

South Australian services available online. The development of the web site was undertaken internally within DAIS. The web site is hosted by an external IT service provider and is managed by DAIS.

The Service SA web site provides a common entry point for all South Australians to access some government related services, information and products, and conduct certain authorised financial transactions.

Audit Findings and Recommendations

Disclaimers

The web site reproduces but does not link to the SA Central disclaimer. The reference to 'this Site' in the disclaimer is therefore appropriate. The language translation disclaimer is particularly appropriate in the context of this web site where a language translation link has been available.

Audit considers that there should be a disclaimer in relation to the availability of the web site and the availability of sites linked from the web site. It should be made clear that it is the responsibility of the user to ensure that all payments or applications for licences are made as required by the relevant legislation regardless of the unavailability of internet facilities.

Ownership of Intellectual Property

Audit was informed that all content including graphics have been internally developed.

A business decision was taken to not register the 'Service SA' name and the accompanying logo due largely to the expense and complexity of this process.

Audit was advised that, in May 2001, advice was sought from the Crown Solicitor's Office regarding protection of the Service SA logo. This followed the discovery that the logo was 'similar' to that used by another company. That company, although operating predominantly overseas, was using the logo in certain retail outlets in Victoria, as well as on its web site. Although the company had trademarked its logo in its home country, no similar application had apparently been made in Australia.

A copy of the advice given on behalf of the Crown Solicitor was reviewed by Audit. It explained the various ways of protecting trade marks, both through registration under the *Trade Marks Act 1995* and also (even in the absence of registration) under the common law of passing off and/or trade practices legislation. However, although concluding that the Service SA logo might be capable of protection through registration as a trade mark, the author did not offer any definitive view as to whether an application for registration would succeed. Instead, it was recommended that further advice be obtained from a trade mark attorney.

Importantly, the advice did not specifically address the risks to the Government in terms of (a) possible legal action from third parties (such as the overseas company) to restrain the Government from using its chosen logo, or (b) the possible 'dilution' of the Service SA brand through other parties (including the overseas company) using a similar logo.

DAIS has advised Audit that following receipt of the advice from the Crown Solicitor, that it would not seek trade mark registration, and did not proceed to obtain the advice of a trade mark attorney.

While Audit recognises that DAIS acted appropriately in seeking advice when it did, and that there may well be good reasons for not seeking trade mark registration, it is recommended that the issue be reconsidered, with a view to addressing the risks identified above.

This might be done by seeking further advice from the Crown Solicitor as to the management of those risks, and whether trade mark registration should be pursued. Apart from matters of legal risk, there is also the matter of the 'reputational/embarrassment risk' of government that is involved in matters of this type.

An important factor in this regard, which was not addressed in the May 2001 advice, is the extent to which the Service SA logo is or is not used outside South Australia. This is significant in terms both of the possibility of the State infringing the rights of those who operate in other locations, and of the extent of the State's own rights to prevent others from adopting similar logos.

It would also be advisable to update the searches undertaken by the Crown Solicitor's Office in 2001 to determine the extent of any use by others of similar marks.

Privacy Policy

There is a link to the privacy statement which applies to the web site. This statement contains a link to the government's privacy statement published by State Records.

The statement also refers to the information collected by the Service SA web site and the use made of such information. The web site consists of links to the service facilities of other service providers.

There is a clear statement in the privacy statement that persons leaving the Service SA web site cease to be protected by the Service SA web site privacy statement. This statement should be reinforced in the process of leaving the web site.

The abovementioned review findings were communicated to the Department for Administrative and Information Services (DAIS) in early 2003.

DAIS Response *— The response from the Department in March 2003 outlined the action being taken to address these matters. In particular, Service SA will modify the disclaimers on the web site in line with audit recommendations and assess issues relating to useability and seamlessness in developing appropriate user warnings on the web site when users leave the site to go to a third party site.*

DAIS advised that Service SA will engage the Crown Solicitor to obtain a definitive answer regarding a Service SA trade mark.

Audit conducted a follow up review in September 2003 seeking an update on the status of the previous Audit recommendations.

DAIS advised in October 2003 that the disclaimers had been updated in line with Audit recommendations. Following advice from the Crown Solicitor's Office, Service SA has applied to have its logo trademarked. This application will be determined in 2004.

CHAPTER 23 — AGENCY REVIEW: COURTS ADMINISTRATION AUTHORITY

INTRODUCTION

The Courts Administration Authority (CAA) was established pursuant to the *Courts Administration Act 1993*. The Authority is constituted of the State Courts Administration Council, the State Courts Administrator and other staff of the Council.

Audit conducted a review of the Magistrates Court Electronic Lodgement Service and the Courts Administration Authority web site.

Audit findings and recommendations were communicated to the Authority in December 2002. The Authority responded in January 2003. Audit conducted a follow up review in September 2003 and the matters advised are reflected in the following commentary.

The IT arrangements in the Courts are, in general, soundly based. In the course of the Audit review certain matters of general interest were identified and these are discussed hereunder.

MAGISTRATES COURT ELECTRONIC LODGEMENT SERVICE

Background

The Magistrates Court Electronic Lodgement Service allows users to lodge general claims, minor civil action claims and pre-lodgement notices in the Magistrates Court jurisdiction.

Audit Findings and Recommendations

Development and Service Level Agreements

There are several agreements in existence for the development, hosting and maintenance of the electronic lodgement system. The primary document is executed between the State Courts Administration Council (SCAC) and an IT service provider.

The development agreement contains standard development warranties in favour of the SCAC in relation to the performance of the product being produced for the SCAC. There are also appropriate confidentiality provisions in relation to information supplied by the SCAC to the developer in order for the web site to be created. The agreement obliges an IT service provider to provide security, in accordance with the reasonable requirements of the SCAC, in relation to both the web site and the software platform for the web site.

The agreement also provides that the intellectual property rights in the electronic lodgement web site are assigned on creation to the SCAC, except in the event of non-payment for services.

There were also two executed service level agreements between the CAA and an IT service provider. These were each valid until 31 December 2002. The agreements were for hosting and administration services for the external CAA web sites and for application support services for the Magistrates Court – Civil Electronic Lodgement System respectively. These agreements are critical to the successful and continuing operation of the web sites and are more fully discussed below.

Parties to the Agreements

The contracting party to the development and hosting agreement, was the 'State Courts Administration Council', a body corporate by virtue of the *Courts Administration Act 1993*.

However the service level agreements for this same project were entered into by the 'CAA'. Section 5 of the 1993 Act provides that the 'Courts Administration Authority' is a collective name able to be given to the State Courts Administration Council, the State Courts Administrator (a position created by the same Act) and other staff of the State Courts Administration Council.

The 1993 Act does not provide that the CAA is a body corporate, or otherwise legally capable of entering into an agreement in that name. It is unlikely that those who drew up the agreements intended that the agreements be between an IT service provider and all of the various bodies and officers for whom the CAA is a composite term. Accordingly, Audit considered that there existed some doubt as to whether the contracts were valid and enforceable. Audit has been advised by the CAA that the State Courts Administrator can enter into a contract on behalf of the State Courts Administration Council, but in the absence of any specific reference to the Council it is not clear that this is what actually occurred in relation to the service level agreements.

The service level agreement for the provision of application support services contains no warranties, indemnities or guarantees. The agreement is limited to a statement of responsibility as between all relevant parties to the maintenance of the web site (CAA, an IT service provider, Bizgate, and EDS) and performance response times and provision for payment. The document is silent as to intellectual property rights created in the course of the provision of the services.

Audit recommended that the CAA review the position and ensure that the appropriate legal entity is named in the new agreements. This has now been done.

COURTS ADMINISTRATION AUTHORITY WEB SITE

Background

CAA provides a web site[19] containing information concerning the operation of the courts system. Its purpose is to be a source of information for the legal profession, general public, and schools, to gain some understanding of the courts system and process, to assist persons who find themselves within the court system to understand what is happening, and to generally keep the public up-to-date about the initiatives being implemented in the courts.

Audit Findings and Recommendations

Disclaimers

The link to the disclaimer on the web site was only visible or accessible from the home page. There was no link from any back page. The disclaimer should be drawn to the attention of the user on each page to ensure that it is accessible to those who, for whatever reason, access the web site directly through a back page.

---

[19] www.courts.sa.gov.au.

The web site uses the standard government disclaimer provided on the SA Central web site. The body disclaiming liability in that disclaimer is the government generally.

Audit recommended that the appropriateness of the disclaimer be reviewed by the CAA to ensure that the disclaimer is appropriate for the web site as a whole and that the disclaimer clearly refers to the CAA web site and not to the SA Central web site. Consideration should also be given to the provision of additional links to the disclaimer from back pages.

CAA Response — *The Authority advised that it will review its web site for inclusion of appropriate disclaimers on relevant pages, and reviewing existing pages where a disclaimer appears.*

CHAPTER 24 — AGENCY REVIEW: DEPARTMENT OF HUMAN SERVICES

OACIS PROGRAMME

Background

The Open Architecture Clinical Information System (Oacis) was designed to provide computer based integrated clinical information. The system stores in electronic form certain information relevant to the clinical care of patients and provides the platform for a comprehensive electronic patient record in the future.

The Oacis system was installed, as a pilot, in 1997, within the renal units of the North Western Adelaide Health Service (The Queen Elizabeth Hospital), Royal Adelaide Hospital, Women's and Children's Hospital and Flinders Medical Centre and subsequently has been installed in three private hospitals.

Approval was given in 2000 for the continuation of the implementation and use of Oacis within the renal units of the above health units, and to extend the use of Oacis, as the common clinical information system, to include all other clinical disciplines within those health units and other nominated hospitals. The additional entities now include the North Western Adelaide Health Service (Lyell McEwin Health Service), Modbury Public Hospital, Noarlunga Health Services and the Repatriation General Hospital.

Audit Findings and Recommendations

Audit's review findings with respect to the Oacis programme are commented on hereunder. These matters were communicated in writing to the Department of Human Services (DHS) in March 2003. The Department responded in May 2003 and that response and, an update in October 2003, are reflected in the following commentary.

Oacis Programme

Audit has been advised that there is no intention to extend the Oacis programme beyond the existing arrangements. Notwithstanding this advice, for the reasons mentioned hereunder, in this review Audit has considered the legal implications of private healthcare providers such as general practitioners and private hospitals being involved with the system.

Firstly, three private hospitals are included in the renal project.

Secondly, Audit has been advised by DHS that there has been some pressure from other sources including the medical profession to expand the programme scope beyond the current public sector use. In my opinion, should that eventuate, there are certain legal risks and privacy issues that would take on increased importance.

Data Quality — Accuracy and Currency

With the introduction of a networked electronic clinical records system, key issues have been identified by DHS in relation to the duty of care owed by individual hospitals to patients. This includes a duty to accurately record and update patient information, and the duty of hospital staff to consider all relevant information when treating a patient.

This issue is not new to networked computerised record keeping. Hospitals and other health care professionals have long faced the risk of liability for negligence if a patient suffered harm due to inadequate or inaccurate information kept in manual paper-based

records systems and single site computer systems.[20] Problems such as inaccurate and missing data, and duplicate records, have always existed with those systems.

The increased sophistication of a networked system, and the increased availability of information that treating clinicians may expect to rely upon, places important obligations on DHS and associated bodies to continue to monitor data quality and undertake regular risk assessments.

It may be that one hospital or health service (Hospital A) enters incorrect information into the system, and a treating clinician in another hospital (Hospital B) relies upon that information. This raises important questions of the liability of the public hospital sector vis-à-vis those private renal dialysis units to which the programme has been extended and vice versa. Any further extension of Oacis within the private sector compounds the risks involved with the necessity for ensuring that adequate risk management arrangements are in place.

If managed correctly, electronic systems have the potential to reduce some of the problems and risks associated with paper-based records systems. However, Audit notes that any failure to implement and manage an electronic networked system to the appropriate standard of care may result in a breach of duty and liability for loss or injury suffered by a patient. Ultimately, the management of this liability for the public hospitals rests with the State. Audit believes it is important that DHS and associated bodies continue to maintain effective management of the system through to its full implementation and operation.

In my opinion, DHS should seek legal opinion regarding the liability of the Government with respect to the private renal dialysis units presently participating in the Oacis programme and ensure that appropriate risk management procedures are observed.

An Enterprise Data Quality Committee (EDQC) has been working with the hospitals on data monitoring and correction processes. The standards that are operative in these matters, in conjunction with other practices and ongoing initiatives, will assist in confirming the identification of a patient, thereby reducing the errors and duplicate records experienced in the early stages of the programme. Under these standards a number of data elements are necessary for the unique identification of a health care client within all health care services. These include: family and given names, date of birth, sex, client unique identifier within the relevant service, and address.

Data quality controls and effective risk assessment processes are important ongoing obligations of DHS and associated bodies. Data accuracy must be closely monitored to reduce the risk that can arise from treating clinicians working with inaccurate patient information.

DHS Response *— The Department advised that it agreed with Audit and continues to monitor data quality issues to ensure accuracy and currency of information available to treating clinicians. Regular risk assessments are undertaken to ensure data quality is maintained as the Oacis System is further implemented within the public hospitals. The Department is committed to this process and proactively addresses data quality.*

The Department advised that it would engage Crown Law to seek legal opinion to deal with liability with respect to private renal dialysis units.

---

[20] See: P MacFarlane, Health Law in Australia and New Zealand, 3rd Ed. 2000, p 197.

Confidentiality

In my Report for the year ending 30 June 2001, Audit outlined the laws governing privacy (also referred to as data protection) and breach of confidence.[21] Privacy will be discussed below. The relationship between a health professional and patient gives rise to a duty of confidence for information that is not publicly known. Health information stored within the Oacis system is clearly protected information. DHS and hospital officers and employees are also under a statutory duty to maintain confidentiality.[22]

Access to patient records must continue to be strictly controlled, and the security of the computer systems and networked communications must be ensured. Staff must also continue to be made aware of their statutory obligations to maintain the confidentiality of patient records. Security that maintains the confidentiality of patient records involves not only protection of the computer system and network, but also control over staff access to and use of that system.

Access to the Oacis system is strictly limited to 'authorised persons' with password access. Varying levels of access are granted depending upon the needs of the user to perform his/her job. All authorised users of Oacis are required to sign an access agreement which includes a confidentiality agreement.

Draft Access Guidelines for the 'Clinical Display Module'[23] were distributed by the DHS in May 2002. The Guidelines, which define access eligibility and the criteria for eligibility, are currently used to assess access requests. Access arrangements for the 'Clinical Order Management Module' (which is currently being piloted) in the Oacis system are still to be developed.

Eligibility for access to the Oacis system for DHS, hospital officers, and employees is conditional upon the user accepting responsibilities for the appropriate use of their username and password, agreeing to comply with the DHS Code of Fair Information Practice, and signing a confidentiality agreement.

Audit believes these procedures are appropriate and DHS should ensure that staff are made aware of their obligations.

The Guidelines also state that authorised users will be required to 're-sign' from time to time to remind and update them about the terms, conditions and obligations of user access.

Audit regards a requirement that users be reminded of their obligations of user access to be of particular importance, and commends this proposal.

Liability for Breach of Confidence

Despite the authorisation process, and requirements that staff accept responsibility for appropriate use of the system, breaches of confidence may still occur.

---

21 Report of the Auditor-General for the year ended 30 June 2001, Part A, pp 169-171 and 174-175.

22 *South Australian Health Commission Act 1976* (SA) section 64.

23 This is a screen-based diagnostic assistance process.

Oacis system use can be monitored with continuous audit trails to detect breaches. The audit trail records what data was accessed, by whom, and when. One of the purposes of the audit trail is stated in a DHS Oacis Security framework document to be to demonstrate that the organisation has implemented proper safeguards if there is a breach of confidentiality. However, the ability to track a breach is not, in itself, proof of adequate safeguarding of data.

If well publicised, audit trails of this kind may well deter deliberate misuse by authorised users and assist in developing a security consciousness in the organisations concerned. Audit trails must continue to be supported by recruiting appropriately skilled staff and providing training and periodic refreshers. These arrangements, properly managed will minimise the risk of a breach of confidentiality.

When combined with well-designed computer, network and user security systems, an audit trail may also provide evidence that demonstrates that a hospital (or the DHS) is not in breach of its duty to patients. However, an employer may still be vicariously liable for the negligent or wrongful conduct of its employees when they are acting within the course of their employment. Audit notes that in the 'Deed of Confidentiality',[24] the private renal dialysis units agree to indemnify the DHS against costs, liabilities etc incurred as a result of a breach of the confidentiality agreement.

Continuing to maintain strict control of user access, and ongoing education of authorised users, is essential to reduce the risks faced by the hospitals and DHS.

DHS Response *— Eligibility for access to the Oacis system for Department, hospital officers and employees is conditional upon the user accepting responsibilities for the appropriate use of their username and password, agreeing to comply with the DHS Code of Fair Information Practice, and signing a confidentiality agreement. This is re-enforced by the 're-signing' of authorised users from time to time against these conditions.*

The Department notes Audit's suggestion of publicising the capability of 'Audit Trails' within the Oacis System to deter any deliberate misuse of information by authorised users. The Department would consider this suggestion and the best mechanism for disseminating this message.

Privacy

As discussed in the Annual Audit Report for the year ending 30 June 2001,[25] South Australia does not have comprehensive privacy legislation. South Australian State Government agencies are required to comply with the Cabinet Information Privacy Principles Instruction.[26] The Department of Human Services has also issued a more detailed Code of Practice based upon the National Privacy Principles (NPPs) in the *Privacy Act 1988* (Cth). These Principles include rules on the collection, storage, use, disclosure, and security of personal information. The DHS Code applies to all Department staff, and all staff of funded service providers including public hospitals. DHS requires that all consultants and contractors, including information technology contractors abide by the Code. The Code states that service agreements with funded service providers and

---

[24] The private renal dialysis units enter into the 'Deed of Confidentiality' as a condition of participation in the Oacis programme.

[25] Report of the Auditor-General for the year ended 30 June 2001, Part A, pp 169-170.

[26] Cabinet Administrative Instruction No 1 of 1989: The Information Privacy Principle Instruction (www.archives.sa.gov.au/services/public/privacy_index.html)

contracts with consultants etc, should clearly set out their responsibilities under the Code.

The intention is to extend the operation of the Code beyond the Department by imposing contractual obligations. Private agencies or practitioners who have access to personal information collected by, or for, the DHS and funded service providers, will be required to observe the Code with signed undertakings. As mentioned above this is done for the private renal dialysis units involved with Oacis in a deed of confidentiality and will be done for any future private sector units.

The DHS Code recognises that with respect to personal health information, private agencies or practitioners may also be subject to the NPPs under the *Commonwealth Privacy Act 1988*. The Code states 'if this is the case, the organisation will need to acknowledge its obligations under that (Commonwealth) Act'. If a private agency is faced with conflicting statutory and contractual obligations, the statutory obligations will obviously prevail.

If additional private health care providers are granted access to the centralised Oacis system, DHS would need to consider any legal and/or operational problems that might arise where users operate under different, or conflicting, privacy provisions.

It is important that DHS continue with current arrangements for there to be a 'Deed of Confidentiality' with all private health care providers, as is presently the case with the private renal dialysis units.

DHS Response *— The Department advised that it had developed deeds of confidentiality in conjunction with the Crown Solicitor's Office for the private renal dialysis units. Should any other private service provider require access then these deeds could form the basis of such an agreement.*

Communication of Confidential Information to Authorised Recipients

As the DHS Code stands, there is limited scope for conflict with the *Privacy Act 1988* (Cth). Nevertheless, there are some differences between the two sets of principles. For instance in the listing of persons 'responsible' for an individual to whom health information may be disclosed in certain limited circumstances, the DHS Code includes, along with other family relationships, a person defined by traditional Aboriginal law, while the equivalent Commonwealth Principle does not.[27] This is an important and commendable addition to the DHS Code. The only comment that Audit makes in relation to this variation is that while relationships such as 'child', 'parent' and so forth are defined in the Code,[28] no assistance is provided to a person implementing the Principle on how they should identify a person defined by traditional Aboriginal law. Explanatory notes are provided for many other Principles in the Code, but not for this one.

DHS Response *— The Department advised that this issue would be forwarded on to the principal authors of the DHS Code for Information Practice for their consideration.*

There are two other areas identified by Audit where there are differences between the Commonwealth NPPs and the DHS Code. These are the Principles dealing with access to, and correction of, personal information, and use of a unique identifier.

---

[27] Subclause 2.5 in the DHS Code and Commonwealth Principles.

[28] Subclause 2.6

Access and Correction

The entitlement of an 'information subject' to have access to, and seek correction of, their personal information is covered by Principle 6 in both the DHS Code and Commonwealth NPPs. The Commonwealth provisions are, however, more detailed. The DHS Code emphasises the importance of entitlement to access, and correction of inaccurate records. However subclauses 6.1 and 6.2 recognise legislative provisions which override the Code, including the Freedom of Information Act.[29] Private health care providers are not subject to freedom of information legislation. The deeds of confidentiality incorporate a requirement in relation to access and amending personal information.

Audit notes that if private users were to be granted access to the Oacis system, they may be operating under different access and correction provisions than the government users. In this situation consideration may need to be given to requiring similar deeds of confidentiality as apply to private renal dialysis units. Given the pressure to make the system available to private users, Audit believes this is an important area that DHS needs to monitor closely.

Use of a Unique Identifier

Principle 7 of the National Privacy Principles under the Commonwealth Act prevents private health care providers from adopting Commonwealth government identifiers (such as the Medicare number) as their own identifier of an individual. The DHS Code of Fair Information Practice also includes Principle 7 relating to unique identifiers.[30] The object of the Principle is to prevent matching of personal information across systems and the likelihood of misuse or inappropriate sharing of data. It is specifically stated that 'while a Medicare number may be used for billing purposes in relation to health services, it should not be used as the basis for another organisation's own identification system'.[31]

With different identifiers in separate systems, the possibility of data matching is reduced. While the Medicare number is the obvious example in the health services context, the principle applies to any unique identifier (usually a number) issued by a Government agency or funded service provider. A person's name is not an 'identifier' for these purposes, and, as the experience of Oacis has shown, is often not unique.

Most privacy principles can be assured by instituting proper collection practices, strictly regulating access, and ensuring security. However, for a networked system designed to share patient information across a range of institutions, good data management potentially conflicts with good privacy practice, at least in relation to Principle 7 restrictions on the use of identifiers. This would emerge as a significant problem if Oacis were extended to private service providers bound by Commonwealth law, and a Commonwealth identifier were adopted for the system, as the Commonwealth Privacy Principles enforce a stricter regime.

While there is potential conflict between the provisions applicable to private health care providers who must comply with the Commonwealth NPPs, and the provisions that apply to users who are governed exclusively by the DHS Code of Practice, so long as a single

29 *Freedom of Information Act 1991* (SA)

30 Department of Human Services, Code of Fair Information Practice, 19 December 2001 (www.dhs.sa.gov.au/finalcodeDec01.pdf).

31 Ibid p 48.

unique identifier is not used across the Oacis system no Principle 7 problems will arise. Again, this is an area which DHS would need to continue to monitor.

DHS Response *— The Department stated that the Oacis system does not rely on a unique identifier for the purpose of linking patients and their clinical test results across the 8 major metropolitan hospitals.*

HEALTHYSA WEB SITE FACILITY

Background

The Department of Human Services (DHS) provides a web site[32] titled 'HealthySA' which became operational in June 2000. The web site is hosted on a DHS computer and is co-located with a commercial Internet service provider.

The web site consists of a series of web site summaries and links provided under a range of specific health-related headings. The purpose of the web site is to provide health information relevant to South Australians. It has brought together all DHS web sites and also provides links to other web sites throughout the world. A wide range of information, which has not been generated by DHS, is therefore available to be accessed by the public from the HealthySA web site.

Audit Findings and Recommendations

Audit's review findings are as stated hereunder. These findings were communicated in writing to DHS in March 2003. The Department responded in May 2003 and that response that was updated as at October 2003, is reflected in the following commentary.

Hosting Agreement

Whilst a set of terms and conditions for hosting services by an external service provider was provided to Audit, they do not name the customer for the arrangement. There is no evidence in the material supplied to Audit that the arrangement has been executed. Without an executed agreement, enforceability of particular terms, conditions and undertakings may give rise to difficulties. That a contractual relationship is in place is not questioned.

The terms are standard terms for services. Audit believes the description of the services to which the terms relate have been accepted in full by DHS, as there is no statement to the contrary in any of the documents provided. The specifications for the terms are stated in a document supplied separately to the terms. The terms disclaim all possible warranties including the availability of any web site and the customer offers a broad indemnity in respect of actions that may be brought against the supplier.

Proper public administrative practice requires that significant contractual relationships be formally documented. This includes the detailing of all terms and conditions and execution by the relevant parties.

---

[32] www.healthysa.sa.gov.au

DHS Response *— The Department responded in October 2003 stating that it was close to finalisation of the new hosting Agreement with the external service provider that hosts HealthySA.*

With respect to disclaimers, DHS advised that Crown Solicitor's Office advice had been sought and changes adopted on the web site.

Disclaimers

There is a disclaimer, that is linked from each of the pages of the web site. This disclaimer states that any medical information provided on the site should not take the place of professional medical advice. This is an important disclaimer. There is a particular need in relation to medical information to ensure that it is not misleading, or that people are not induced to rely on information that is general and that has the potential to cause personal harm if interpreted or applied incorrectly.

While the disclaimers used are commendable, Audit is of the view that further emphasis should be made on the home page of the web site that the information available is general information and that for specific advice a medical professional should be consulted.

The higher the potential risk, the more prominent any disclaimer should be. As the information being provided is medical information, the inherent risk is by its nature high. In these matters disclaimers should be easy to access and prominently displayed to the user of the web site.

DHS Response *— The Department advised that the HealthySA Privacy Statement would be updated in line with the recommendations made by Audit.*

Ownership of Intellectual Property

Audit was advised by DHS that the web site was largely developed within DHS and that an external contractor had assisted with the interface design and the creation of the logo which appears on the web site. The arrangement for the development and the ownership of any intellectual property rights in the structure of the web site or its initial content was never fully documented. The agreement with the host states that the customer is responsible for the content of the web site, implying that the provider does not own any rights in such material.

As a matter of prudent administrative practice DHS should clarify ownership of all intellectual property rights and, in particular, any potential external ownership, and take any necessary action to confirm these rights.

DHS Response *— DHS have taken steps to address matters relating to ownership of intellectual property.*

Linking

'The Principles of Publishing' page, which appears on the web site, refers to submissions of content links being assessed by registered assessors.

The HealthySA Reference Group (the registered assessors) is responsible for the assessment of content links and for information on the HealthySA web site. Members of the HealthySA Reference Group may or must (it is not clear which) register to be

submitters or approvers of material for the web site. The Group member registers in a content category in which the member is 'qualified' to submit and/or approve.

There is no indication to a user of whether this 'qualification' is self-assessed or whether the application for registration is itself assessed by an independent person. This is an issue of transparency. However, there is also a legal risk in that the persons making the assessment are stated to be 'qualified'. If this is not the case, and the assessor has no formal qualifications or has inappropriate qualifications, then this may amount to misleading conduct on the part of HealthySA to promote persons with no qualifications as persons who have qualifications. If members of the public are induced to rely on a linked site as a result of the recommendation of the assessor, HealthySA could be exposed to a liability risk. Nor has any information been provided as to the identity of the persons who perform the role of assessing submissions, or as to the precise qualifications required of or actually possessed by them.

There is no information available on the HealthySA web site as to the process of registration of assessors. This is primarily an issue of transparency to reassure the users of the web site as to the qualifications of the persons assessing the links available on the web site. Audit believes this would be a useful addition to the site.

While some information has been provided as to the process of 'accreditation' (in as much as accreditation involves nominating to be an assessor), there is no information which would reassure the public as to the genuine qualifications of the persons approving any material submitted for approval to the web site. Similarly, Audit believes this would be a useful addition to the web site.

DHS Response *— The Department stated that it would include this information in the Principles document published on the HealthySA web site.*

Privacy Policy

The privacy statement notes that if DHS is contacted through the 'contact us' facility, the e-mail address will be retained and the information will be passed to the person best able to assist in answering the message. It is noted that this person may not be within DHS. There is a statement that the information provided would only be used for the purposes for which it was provided. If information is being passed outside DHS, the recipient of the information may well, (depending on whether they are in the public or private sector), be obliged to comply with either State government policy in relation to privacy or the *Privacy Act 1988* (Cth).

There is no indication in the privacy statement as to the level of security associated with the submission facilities of the web site. There is also no statement as to how a person can access information held by HealthySA or DHS (via HealthySA web site facilities). These are both recommendations of the Privacy Committee of SA's Privacy Guidelines for South Australian Government World Wide Web sites.[33] Audit would suggest these recommendations be applied by DHS.

DHS Response *— DHS stated that the privacy statement had been updated in line with Audit recommendations and in consultation with the DHS Privacy Officer.*

---

[33] www.archives.sa.gov.au/services/public/privacy_index.html.

CHAPTER 25 — AGENCY REVIEW: DEPARTMENT OF TRANSPORT AND URBAN PLANNING — TRANSPORT SA

REGISTRATION AND LICENSING INITIATIVE

Background

Transport SA (TSA) and EDS (Australia) Pty Ltd (EDS) have developed an e-commerce service for a range of motor vehicle registration and driver licensing transactions.

The new TSA e-commerce system makes available 25 transaction types to be conducted via the Internet. These include transactions such as:

- registration quotes and renewals;
- modification of registration details and transfers;
- licence details and driver offence history enquiries;
- enquiries and the recording of interests for the vehicles securities register.

Transactions requiring payments will be payable by credit card or direct debit.

The implementation date of the e-commerce facility was mid 2003.

Audit Findings and Recommendations

Audit's review findings are commented on as follows and were communicated in writing to TSA in November 2002. TSA responded in March 2003. The position has now been updated to September 2003. The matters advised are reflected in the following commentary.

Audit found that liability for data integrity and privacy have emerged as matters that give rise to control inadequacies. Certain other potential legal issues also warrant comment. A matter of particular interest arises with respect to the application of stamp duty to transactions conducted using the e-commerce facility.

Internet Access by Members of the Public

The original specifications for the e-commerce system were subsequently revised so that the general public will only be able to execute registration renewals, change address details, enquire about registration fees, provide disposal notices, and order replacement plates. TSA advised Audit that the general public would not have user id's and passwords. Initiation of transactions would require a level of user identification from certain documentation, eg (dependent on the transaction) a payment number, plate number, client number or driver's licence number.

As long as authentication of the user can be assured, electronic enquiries about personal information should not present privacy problems.

Depending upon how the system is developed, change of personal information (such as home address) might be seen as data entry in the sense discussed below. However, entries of this kind could equally be seen as simply notices of changes as required under the *Motor Vehicles Act 1959* (SA), and as currently provided over the counter, by mail, e-mail or phone. This level of public access seems to present few legal problems so long as the security systems operate to an appropriate standard.

Transport SA Response *— The general public would not be able to access any personal information through the E-Commerce facility, only having access to limited transactions and would need to enter a number of identifiers before proceeding with a transaction.*

Other external users and agents will have access to a greater range of transactions and would be required to enter user ids and passwords in addition to entering key identifiers for each transaction. This would allow for authentication of the user and all transaction information would be logged against this user for future reference and auditing.

Data Entry by Motor Vehicle Dealers and Others

The system specifications delegate certain powers in the vehicle registration process to new and used motor vehicle dealers, fleet owners, local councils, insurers, and transport operators. These include new registrations, transfers, cancellations, and ordering replacement plates. With respect to these matters information is entered onto the system by the dealers and other users.

Financial institutions are also delegated powers for lodgements in relation to the Vehicle Securities Register (VSR). These 'delegates' might be considered to be acting as agents of TSA in the data entry process. External agents and operators (other than the general public) will be identified on the system and each transaction will be traceable.

Certain legal issues arise in this context ie, (1) the risks associated with the entry of inaccurate data and other matters; (2) stamp duty matters and certain other matters concerning electronic transactions.

Risks of Inaccurate Data Entry by Delegates and Other Matters

Under the Act, the Registrar may delegate his or her powers to specified persons or bodies of persons that, in his or her opinion, have appropriate qualifications or experience.[34] This must be done in writing.[35]

'Primary delegates' are entities such as motor vehicle dealerships whose staff or agents will be 'employee delegates'. Delegates are required to enter into a Deed of Agreement with TSA.

The deed imposes a range of obligations upon the primary and employee delegates. The question arises however: what risks does TSA face if the delegates act wrongly or negligently? Data may be entered wrongly, or source documents may not be correctly maintained, resulting in loss by a member of the public. Further, notwithstanding the strict obligations imposed by the deed, driver or registered owner confidentiality may nevertheless be breached.

Persons engaged in the administration of the Act are protected from liability for honest acts or omissions.[36]

The risks of inaccurate data entry and other breaches by delegates may be reduced by close monitoring of the use of the system. The deed requires delegates to maintain source documents and submit to audits by the Registrar.

Audit considered this to be an important control provision to maintain the integrity of the system.

---

[34] *Motor Vehicles Act 1959* (SA) section 7(4)

[35] *Motor Vehicles Act 1959* (SA) section 7(6)

[36] *Motor Vehicles Act 1959* (SA) section 139E.

Stamp Duty and 'Writing' Requirements

Stamp duty is payable on most compulsory third party insurance policies. This is paid at the same time as the registration renewal. Under the stamp duties legislation, duty attaches to an 'instrument'[37] which is defined to include 'every written document'. This is, in turn, defined to include 'every mode in which words or figures can be expressed upon material', and material means 'any sort of material upon which words or figures can be expressed'.[38] Although this is an inclusive definition, the reference to 'words and figures' being expressed 'upon' material does not readily encompass an electronic transaction.

It should be noted that the recently proclaimed *Electronic Transactions Act 2000* (SA) was passed to facilitate the use of e-commerce transactions. It has the effect that where the law requires 'writing' for a valid transaction, that requirement is taken to have been met by the use of electronic communication or storage in a range of circumstances.

However, in advice provided to TSA, the Crown Solicitor's Office has suggested that these provisions will not thereby make an electronic communication a 'written' instrument for the purposes of stamp duty. The argument appears to be that the legislative provision which imposes stamp duty on instruments does not constitute a 'requirement' that information be given or recorded in writing. On the face of it, that advice would appear, as a matter of logic, to be soundly based.

TSA has advised that current processes still require written instruments to be completed and forwarded to Registration and Licensing. So long as a paper based system is maintained alongside the electronic system it seems that the stamp duty problem will be avoided. However, a time may come when TSA wishes to implement a fully electronic system.

In this regard, TSA indicated that advice was being sought on possible changes to the Stamp Duties Act.

Transport SA Response *— New and used Motor Vehicle Dealers would still be required to ensure that appropriate applications are completed correctly prior to undertaking transactions electronically via E-Commerce. The forms would be forwarded to Registration and Licensing for quality control checks to ensure correct completion of the application and entry of data. All forms would then be stored in line with existing audit requirements applicable to forms lodged at Customer Service Centres. Therefore, a written instrument" would exist for determining stamp duty on value of the vehicle.*

Electronic Transactions Act and Regulations

When giving advice on the proposed system in 1998, the Crown Solicitor also expressed an opinion that provisions in the *Motor Vehicles Act 1959* requiring the submission of notices, applications, and other information in writing or with signatures (for instance when ownership of a motor vehicle is transferred, or when there is a change of address) could not be satisfied electronically.

TSA will need to bear in mind that the Electronic Transactions Regulations 2002 exclude from the operation of the 2000 Act any requirement that a document be witnessed.

---

37 *Stamp Duties Act 1923* (SA) section 4

38 *Stamp Duties Act 1923* (SA) section 2.

Thus where for example there is a requirement to supply a statutory declaration in support of a particular application or notification,[39] that requirement will not be able to be met electronically, unless the legislation imposing the requirement itself specifically allows for such an arrangement.

Again, this may not be a problem while full paper records are also required to be maintained. It would, however, become an issue with any shift in the future to a fully electronic system.

Transport SA Response — *Where there is a requirement to supply a statutory declaration in support of an application, delegates would need to keep a paper copy of both the application and the statutory declaration. The general public would not be able to electronically process transactions which will require a statutory declaration.*

---

39 See eg *Motor Vehicles Act 1959* section 44(1a) concerning notifications of additions or alterations to vehicles.

CHAPTER 26 — AGENCY REVIEW: DEPARTMENT OF TREASURY AND FINANCE — REVENUESA

INTRODUCTION

RevenueSA, a branch of the Department of Treasury and Finance (DTF), is responsible for the collection and enforcement of the State's taxation revenue base. This includes a range of licence fees, stamp duty, payroll tax, and the fixed property component of the emergency services levy.

As commented in my 2001 Report, e-commerce can pose problems for the tax base of State governments when the relevant jurisdiction for a transaction is difficult to identify.[40] While this is unlikely to be a problem for the Emergency Services Levy based upon fixed property, for revenue such as stamp duty which is based upon a wide variety of 'instruments', the relevant jurisdiction for e-commerce transactions and the 'location' of intangible property raise difficult questions.

On a more basic level, the current stamp duty legislation may not cover 'exclusively' electronic transactions. This matter needs to be resolved as the range of exclusively electronic transactions (with no paper based documentation supporting them) is likely to increase with the expanding use of e-commerce.

Audit's findings and recommendations with respect to Payroll Tax Collections, RevenueSA web site and the RevNet Project were communicated to RevenueSA in December 2002. RevenueSA responded in January and February 2003. The position has been updated to September 2003. The matters advised are reflected in the following commentary.

PAYROLL TAX COLLECTIONS

Background

Lodgement and payment of Payroll Tax returns can be made by registered users via the Internet. Payments are made by direct debit to a pre-nominated bank account.

The RevenueSA webpage contains a link to this site that is located at Bizgate, the South Australian Government e-commerce initiative managed through the Department for Administrative and Information Services (DAIS).

Audit Findings and Recommendations

In the Report for the year ending 30 June 2001 Audit noted that there were a number of client agencies without formal agreements with Bizgate.[41] As a basic administrative practice, documentation needs to be put in place for all service-based arrangements. Documentation should, inter alia, cover areas such as service levels, continuity of operations, intellectual property rights, and required security controls.

Agreements for the operation of the Payroll Tax payment system between RevenueSA and DAIS, are, as at the date of this Report, yet to be established.

Even though both are government agencies, agreements setting out the responsibilities and obligations of each party should be formalised. This allows for responsibility and

---

40 Report of the Auditor-General for the year ended 30 June 2001, Part A, p 164.

41 Report of the Auditor-General for the year ended 30 June 2001, Part A, pp 188-189.

accountability to be clearly understood. Where there is no documentation, there is the potential for misunderstandings between the parties about the level of service that is to be provided. In these circumstances there is a risk that service delivery to the public may be compromised.

Responsibility for continuity of operations, testing, implementation and documentation of significant system changes, and ownership of intellectual property, are some of the matters that should be addressed in a formal service level agreement.

Department Response *— In September 2003, Audit was advised that discussions had commenced with DAIS regarding establishment of a service level agreement, but this had not yet reached a stage of finalisation.*

REVENUESA — WEB SITE

Background

The RevenueSA web site[42] is one component of the Department of Treasury and Finance (DTF) Internet site. It contains information about RevenueSA and the legislation administered. This web site contains a capacity to link to RevNet through which certain financial transactions can be made. RevenueSA staff administer and review the content of the Internet site on a regular basis.

Audit Findings and Recommendations

Hosting Agreement

There is a hosting arrangement in place between the host and DTF. The government party to the agreement is not made clear, and the copy of the agreement provided to Audit had not been executed on behalf of any government agency.

The terms are standard terms for a hosting agreement. It is a condition of the arrangement that the host does not review web site material and takes no responsibility for any information displayed on any web site hosted.

The renewal of hosting services for the current year refers to maintenance and support services supplied to DTF. It is not clear from the information provided what those support services consist of and whether it involves any development and/or modification of the web site itself.

There are no intellectual property rights provisions in the terms provided. If the support services include services in relation to the web site, it is possible that such services include the creation of intellectual property rights which might then be the property of the supplier as there is no agreement to the contrary.

The hosting arrangements provided for Audit review state that the host of the web site takes no responsibility for the content of the web site and security access is arranged so that the customer (DTF) can make alterations to the content of the web site. This implies that the content of the web site is not owned by the host but by DTF, which is confirmed by the copyright statement on the web site.

It should be ensured that if any support services in relation to the web site are being provided by a third party supplier, that there are adequate intellectual property rights

---

[42] www.revenuesa.gov.au

provisions in place so that the ownership of intellectual property rights in the web site remains with the relevant arm of government.

Department Response *— While the current hosting agreement with the host does not expressly refer to intellectual property rights, the understanding between that organisation and Treasury and Finance was that the Government owns these rights. As this arrangement was to be reviewed, specific clauses relating to intellectual property would be incorporated into any new agreement negotiated with the new hosting service.*

Disclaimers

The web site uses the standard government disclaimer provided on the SA Central web site by redirecting the user to that particular site. The disclaimer is a government approved (minimum) disclaimer for use where applicable by government agencies. The disclaimer seems to cover all issues likely to be raised by the provision of information to the public, and in particular, contains a disclaimer as to the accuracy of information supplied.

The supplied disclaimer does, however, refer to 'this web site'. As the SA Central web site is at a different location and a screen is displayed indicating that clicking on the link to the disclaimer involves being redirected to another site, there is a risk that the disclaimer will be interpreted as not applying to the RevenueSA web site but only to the SA Central web site.

Alternatively, the text of the SA Central web site disclaimer could be reproduced on the RevenueSA web site so that the references to 'this Site' are accurate, and the references to the Government of South Australia may need to be reviewed. The named entity should be the legal entity which is responsible for the web site. If this is a department of State, the reference to the Government of South Australia is appropriate. The disclaimer should also be reviewed, particularly in circumstances where a new function is added to the web site, to ensure that any additional risk created by the new function is added to the disclaimer where appropriate.

The disclaimer does not include a disclaimer as to the availability of the web site. As this is a warranty which is expressly excluded in the hosting arrangement, it should also be excluded by RevenueSA in some form.

Department Response *— The disclaimer used on the web site is the Whole-of-government disclaimer which was required to be used under government policy. Any change to the disclaimer would need to occur at a whole-of-government level.*

Circulars

Circulars are information sheets issued by RevenueSA containing information for consumers concerning changes to legislation administered by RevenueSA or changes to administrative practices or procedures. Links to the published circulars are available on the web site. These circulars do not carry copyright statements but do bear the letterhead of RevenueSA. There is no reason why copyright notices should not appear on such circulars to emphasise the fact that copyright is claimed and that there may be conditions attaching to the use of such circulars. If there are any such conditions (including a licence to print the circulars for personal use, a prohibition on reproducing circulars etc), then these terms should be identified and drawn to the attention of the user.

As RevenueSA offers the circulars to the public as information about the calculation of stamp duty, RevenueSA should have procedures for ensuring that the circulars which are available through the web site are accurate and up-to-date. Having such procedures will minimise the risk that the circulars will offer information which is no longer correct and which might cause a user to suffer detriment if such outdated information were relied upon. This principle also applies to all other information on the web site. Appropriate disclaimers should again appear, noting that the information is provided as general information only.

Department Response *— In September 2003, Audit was advised that the Information and Administrative Services Branch of Department of Treasury and Finance is addressing RevenueSA web site recommendations. A disclaimer has now been attached to all RevenueSA web site components.*

Ownership of Intellectual Property

If RevenueSA does not own the intellectual property rights in the material which comprises any developments, maintenance or upgrades to the web site, RevenueSA may be restricted to the creator of the intellectual property for further maintenance, upgrades and developments. It may amount to copyright infringement if any of these functions are carried out by any person other than the creator or a person authorised by the creator. RevenueSA should ensure as far as possible that it owns the rights, or has a written licence which permits any third party to carry out these functions.

There is some doubt as to the status of intellectual property rights in anything done by the host for the purpose of maintaining and supporting the web site.

Department Response *— While the current hosting agreement with the external service provider does not expressly refer to intellectual property rights, the understanding between that organisation and Treasury and Finance was that the Government owns these rights. As this arrangement was to be reviewed, specific clauses relating to intellectual property would be incorporated into any new agreement negotiated with the new hosting service.*

REVNET

Background

An Internet based system called RevNet,[43] has been developed by RevenueSA.[44] This system allows for self-assessment and the electronic lodgement of data and payments for revenue collection through the internet.

Audit Findings and Recommendations

Contractual Arrangements

The RevNet system was developed 'inhouse' by RevenueSA.

An interim web-hosting agreement has been negotiated with EDS. The services to be provided by EDS include IT hardware and support, software licences and support, and Web hosting Services not included within the scope of the ITSSED agreement (Information Technology Services and State Economic Development Agreement)

---

[43] Formally called eSARD - electronic Self-Assessment of Revenue relating to Documents.

[44] www.revenuesa.sa.gov.au/revnet.html

between the State and EDS. The interim agreement was signed in August 2002 with the intention that it be reviewed after three months. At the time of preparation of this Report, the full agreement had not been signed and the interim agreement had been extended.

The need for full documentation for web-hosting agreements has been raised with a number of agencies by Audit and is the subject of comment with respect to other matters in this Report.

The terms of the interim agreement basic. The terms list the fees to be paid and include an undertaking by EDS to perform the services detailed in its proposal dated 25 March 2002.

Proper public administrative practices necessitate that this agreement should be finalised as a matter of priority. As Audit has highlighted in previous reports,[45] agencies may incur significant risks by proceeding with this type of project without appropriate contractual underpinning.

Approval of Special Tax Return Arrangements

The *Taxation Administration Act 1996*[46] contains special provisions that allow the Commissioner of State Taxation, by written notice, to approve special arrangements for the lodging of returns and payment of tax for a specified taxpayer or class of taxpayers. This includes the lodging of returns and payment of tax by electronic means. An 'Approval' by the Commissioner given under these provisions is binding on the relevant taxpayers. An Approval by the Commissioner relating to stamp duty may exempt a requirement for the stamping of an instrument and allow instead for the endorsement of that instrument.[47]

In October 2002 RevenueSA produced a document titled 'Approval of A Special Tax Return Arrangement including Internet Terms of Use'. This document incorporates an Approval by the Commissioner for self assessment using the RevNet service. The terms and conditions of use are agreed to with the signing of the Approval document, however, RevenueSA reserves the right to amend the terms at any time by publication on the web site. Use of, and or access to, the RevNet site is taken in the Approval document to constitute acceptance of the terms of use including any amended terms.

It is arguable that this method of varying the terms and conditions under the Approval does not accord with the statutory requirements in sections 38 and 38A of the Act. This is a matter that should be clarified by seeking an authoritative opinion from the Crown Solicitor.

Under those provisions a written notice of variation may be made by either publication in the Gazette, or service of the notice on the relevant taxpayer or agent.[48]

Department Response *— RevenueSA agreed to seek advice in line with Audit recommendations.*

---

45 See for example Report of the Auditor-General for the year ended 30 June 1998, Part A, pp 79-80

46 *Taxation Administration Act 1996* (SA) section 35

47 *Taxation Administration Act 1996* (SA) section 40

48 *Taxation Administration Act 1996* (SA) section 38A.

Approved Person

An approved 'person' (which might be a corporation) may nominate a list of natural persons who will have access to RevNet. The Approval enables these persons to 'self determine', that is, to assess for themselves the stamp duty to be paid, and arrange to do so by electronic return using RevNet or, if the system is unavailable, by Periodic Return Arrangement (PRA). Self assessment will be done using a RevenueSA Stamp Duty Document Guide. The Approval by the Commissioner includes exemptions from various provisions in the *Stamp Duties Act 1923*[49] to facilitate electronic lodgement via RevNet.

As already discussed above in Chapter 24, on a more basic level, the current stamp duty legislation may not cover exclusively electronic transactions.

Department Response — *Cabinet approval was granted on 25 November 2002 for the Stamp Duties Act to be amended. Discussions have been held with Parliamentary Counsel officers who are in the process of drafting appropriate legislative amendments.*

---

49 *Stamp Duties Act 1923* (SA).