[P.P.4H

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 2005

Tabled in the House of Assembly and ordered to be published, 30 November 2005

Fourth Session, Fiftieth Parliament

Supplementary Report

Government Management and the Security Associated with Personal and Sensitive Information

By Authority: K. O'Callaghan, Government Printer, South Australia

2005

Government
of South Australia

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: audgensa@audit.sa.gov.au
Web: http://www.audit.sa.gov.au

ABN: 53 327 061 410

29 November 2005

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

The Hon R Such, MP
Speaker
House of Assembly
Parliament House
ADELAIDE SA 5000

Gentlemen,

Auditor-General's Supplementary Report: Government Management and the Security Associated with Personal and Sensitive Information

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 'Government Management and the Security Associated with Personal and Sensitive Information'.

Yours sincerely,

K I MacPherson
AUDITOR-GENERAL

Supplementary Report: Government Management and the Security Associated with Personal and Sensitive Information

TABLE OF CONTENTS

Supplementary Report: Government Management and the Security Associated with Personal and Sensitive Information

TABLE OF CONTENTS

EXECUTIVE SUMMARY

INTRODUCTION

A Supplementary Auditor-General's Report to Parliament in December 2003 titled 'Information and Communications Technology — Future Directions: Management and Control', highlighted several weaknesses in the security and control arrangements of agencies' computer systems and computing environments that had been subject to audit review.

Since presentation of that Report audits of computer systems and computing environments continue to be undertaken as part of the annual statutory audit process of public sector agencies. The audits in 2004-05 included focussed attention to three systems associated with processing and storage of information of a personal and sensitive forensic and medical nature.

The three systems reviewed were the CaseMan System and the SACREDD DNA System operated by Forensic Science SA of the Department for Administrative and Information Services (DAIS), and the ULTRA Pathology System operated by the Institute of Medical and Veterinary Science. The SACREDD System is of critical importance in the administration of the justice system in this State.

IMPORTANT ISSUES OF PRINCIPLE AND PRACTICE IN PUBLIC ADMINISTRATION

The computer system audits in 2004-05, particularly the three abovementioned system audits, raised certain important issues of principle and practice with respect to public administration in this State. These issues relate to government agencies complying with the law, agencies working together effectively for the public benefit, and agencies ensuring that effective security and control is exercised over computer systems and information.

This Report explains these issues of principle and practice in the context of the audit findings arising from the audits of the three abovementioned computer systems and computing environments.

SPECIFIC MATTERS REVIEWED

The audits of the three systems were directed to obtaining an understanding of the governing requirements for system operations and the key personnel involved with the systems. In addition, an assessment was undertaken of aspects of security and control over computer systems and computing environments, including access authorisation, protection over the custody and use of system information, and system continuity planning arrangements.

In undertaking the assessment, particular regard was had to the agencies' compliance with the requirements of the Government's Information Security Management Framework (ISMF). This framework establishes minimum security standards and guidelines for implementation by public sector agencies.

SUMMARY OF REVIEW MATTERS CONTAINED IN THIS REPORT

Compliance with Law

It is important that agency Chief Executive Officers and senior management understand the legislative framework in which they operate and that they implement processes to ensure compliance with that framework. Furthermore where the requirements of legislation may not be absolutely clear that expert legal advice be sought to enable proper processes to be implemented to provide compliance with matters that may be mandated by legislation.

In regard to the SACREDD DNA database system, its configuration and use are governed, in most part, by requirements contained in the *Criminal Law (Forensic Procedures) Act 1998*.

The audit identified issues that, in my opinion, were not in strict compliance with the relevant statutory requirements and certain matters where there was the need for legislative clarification . The first mentioned matter related to the destruction and removal of DNA profile information from the system and associated records. The latter matter related to issues of recording on the database of DNA profile information for Forensic Science SA staff and 'known deceased persons', and the use of deceased suspects blood samples.

Agencies Working together for Effective Outcomes

In recent years, agencies of government have in some instances been required to work together for the purpose of undertaking a shared responsibility and/or response to achieving an effective outcome(s) in relation to a government policy initiative(s). This situation applies in relation to the SACREDD DNA database system which involves multi-agency involvement comprising the Police Department, DAIS and Forensic Science SA, and the Crown Solicitor's Office. EDS Pty Ltd also provides processing, storage and restoration services in relation to the system.

In order to achieve optimum 'connectedness' between the agencies and therefore effective outcomes, responsibilities and accountabilities of the agencies need to be clearly understood, and the quality of cooperation (including in matters of communication, responsiveness and decision-making) need to be of a high order.

The audit review identified issues that, in my opinion, were in need of consideration to enhance the effectiveness of the working relationship between the participating parties. These matters related to improving aspects of the formalised administrative arrangements between the parties, enhancing policy and procedure matters for application by the parties, and revisiting quality assurance and audit arrangements. The matter of the effective coordination of legal advice regarding areas of operational complexity also, in my opinion, required examination.

Improvement in Security and Control Arrangements for Computer Systems and Information

The Government, through its many agencies, uses computer information systems to process, transmit and store information critical to the performance of its key business operations including core governmental services and financial outcomes. Of necessity, there should exist the highest standards of security and control over these systems and the information held by them. Certain information maintained on systems and databases can be classified as personal and sensitive, as is the case in relation to the three systems that were the subject of focussed review.

The audit identified many issues in relation to the three systems that, in my opinion, presented risks of unauthorised access to the systems and information, and to the confidentiality, integrity and availability of the systems and information. In this respect, a number of the issues fell short of the ISMF minimum standards for security and control measures that are now mandated as government policy.

Chief Executives are responsible for security within their agencies. It is important that an ongoing review program is undertaken within each public sector agency to ensure systems and related security and control measures meet the minimum standards set out in the ISMF.

AGENCIES' RESPONSES TO THE AUDIT MATTERS RAISED

The matters identified in this Report were communicated in Audit management letters to the respective agencies and formal responses to those matters were received from the management of the agencies.

In an overall context the agencies have acknowledged the validity of the matters that were in need of addressing. In this regard the agencies have either taken or indicated appropriate planned corrective action.

The positive nature of the agencies' responses and corrective action is illustrated in one particular communication from the Chief Executive, DAIS, stating '… we are entirely committed to addressing all the matters raised and have made sincere and rigorous endeavours to ensure these matters are and will continue to be addressed'.

CONCLUDING COMMENT

This Report emphasises the need for agencies to exercise vigilance in ensuring adequate management and security arrangements are in operation in relation to their computing systems and computing environments.

1. CONTEXT OF AUDIT REVIEW

1.1 Purpose of Audit

Individual agencies of government are responsible for the development and/or operation of a range of computing systems that are of major public interest importance. These systems deal, inter alia, with a number of areas of government service delivery and financial operations.

The effective management, security, and the control of agency 'computing systems' and their respective 'computer processing environments' are important for ensuring the completeness, accuracy, and validity of the information that is produced and/or maintained by those systems. It is this information that underpins the overall integrity of operational decision-making, service delivery, and the financial accountability obligations of the agency.

As part of the 2004-05 annual audits of computing systems and computer environments, three systems were reviewed. These systems are the:[1]

- CaseMan system;
- SACREDD system; and
- ULTRA system.

These can be characterised as systems that process and store personal and sensitive forensic and medical information. One of the systems, ie the SACREDD system, is of critical importance in the administration of justice in this State. With respect to this system, its configuration and operation is prescribed by legislative requirements. The other two systems are of major public importance in the context in which they operate.

1.1.1 The 2003 Supplementary Auditor-General's Report

In December 2003, I presented a Supplementary Report to the Parliament titled 'Information and Communications Technology – Future Directions: Management and Control'. That Report, highlighted some notable weaknesses in the security and control arrangements of agencies' computing systems and computing environments that had been the subject of audit review.

The December 2003 Supplementary Report also mentioned that a new 'Information Security Management Framework' (ISMF) was being introduced by government. This framework documented the up-to-date Information Technology security standards and guidelines that were required to be implemented by agencies in relation to their respective computing systems and infrastructure.

Since tabling of the Supplementary Report in December 2003, audit reviews continue to be undertaken of agencies' computing systems and environments, as part of the 'control' and 'financial attest' components of the annual audit process applied to agencies' operations. The various outcomes of these audit reviews are, where applicable, the subject of separate commentary in the sectional agency reports presented in Part B of my annual Report to the Parliament.

---

[1] The three systems reviewed were the SACREDD DNA system and the CaseMan system operated by Forensic Science SA of the Department for Administrative and Information Services, and the ULTRA Pathology system operated by the Institute of Medical and Veterinary Science. In relation to the SACREDD DNA system, the Commissioner of Police is vested with statutory responsibility for the system. However, key aspects of its operations have been delegated by the Commissioner of Police to the Director, Forensic Science SA.

1.1.2 2004-05 Audit Reviews

The audits undertaken of agency systems in 2004-05, particularly the reviews of the three systems referred to above that are associated with personal and sensitive information, raise certain important issues of principle and practice with respect to public administration in this State. The issues include the importance of government agencies complying with statutory requirements; agencies ensuring that effective security and control is exercised over the storage and processing of information; and agencies working together effectively for the public benefit.

This Report explains the issues of principle and practice that are associated with the audit findings that are referred to in this Report.

1.2 Important Principles for Government in Managing and Controlling Personal and Sensitive Information

1.2.1 Compliance with the Law

Agencies of government carry out their responsibilities within a legislative and policy framework. In certain instances mandated legislative provisions govern the structure and process by which an agency conducts some or all of its affairs.

It is important that Chief Executive Officers and agency senior management clearly understand the statutory framework within which they are required to discharge their responsibilities. They are also required to be conscientious in ensuring that the agency functions and operations are conducted according to law and the legitimate policy directions of the Executive Government.

1.2.1.1 Claims of Administrative Inconvenience

A view may sometimes be put forward by an agency or officers within an agency that, given certain situations or circumstances, it can be administratively burdensome, difficult, or inconvenient, or not cost effective to comply in strict terms with a statutory requirement. Where the object and purpose of an Act of Parliament is clear and unambiguous there is no room for non-compliance. Claims of administrative difficulty and/or inconvenience are no excuse for non-compliance in these circumstances.[2]

1.2.1.2 Compliance with Mandated Policy Framework

The ISMF is a formal South Australian Government Policy Directive. The ISMF is the standard by which Executive Government agencies in this State are to be held accountability for those matters that are required to be dealt with in the framework document.

In April 2003, the ISMF was approved as the minimum information technology security standards and guidelines for implementation by agencies.

---

2 As discussed herein in this Report, a specific requirement can be prescribed in statute relating to the destruction or retention of information of a personal or sensitive nature that may be held by an government agency. The statute may dictate destruction of the information forthwith on the basis of a prescribed condition(s). The Legislature, in this instance, has determined that the protection of the citizen's anonymity is of overriding importance in those circumstances where the condition(s) of destruction exist. It is the requirement of the Parliament that the government agency establish and implement an administrative process or procedure to enable destruction of the information in accordance with the statutory requirements.

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 with respect to these matters.

The ISMF sets clear objectives in respect of the application of the framework. Those objectives are essentially to:

- provide a data classification and risk assessment process to identify information assets and the level of risk associated with these assets;
- apply appropriate security controls to permit the efficient and secure access to information assets;
- obtain assurance on an annual basis as to the effectiveness of agency information security measures;
- provide protection for the privacy and confidentiality of SA Government clients and any information that government keeps about members of the public;
- ensure that there is a high level of awareness and commitment to information security requirements.

1.2.2 Obligation to Ensure Security and Maintenance of the Confidentiality of Personal and Sensitive Information

Government agencies, in undertaking their operational objectives and financial accountability obligations, process and store a diverse range of information on computing databases and systems.

Certain of the information maintained on the databases and systems can be classified as personal and sensitive. In most instances, it is used to facilitate the effective provision of service delivery to members of the community, or to enable performance of policy and corporate functions, or for purposes of undertaking law and order functions of government.

It is an important responsibility of government agencies to ensure that adequate security and control mechanisms are in place to prevent unauthorised access to systems and information. Inadequate safeguards can result in adverse financial and other consequences for government and for members of the community.

This important matter of security and control over information access is recognised in the Government's ISMF. This framework requires agencies to risk assess their data and then implement appropriate security and control measures on the basis of that assessment. This is in order to ensure adequate protection of information and the prevention of adverse consequences.

1.2.3 Procedures and Processes of Government Agencies must not Undermine Public Confidence in the Institutions of Government

The matters of compliance with law and the implementation of government policy with respect to security over information and assets are important areas of public administration. Inadequacies or failures in the administrative arrangements in relation to these matters can undermine confidence in the processes of government.

A further area of importance relates to developments in recent years of agencies working together for the purpose of achieving public benefit outcomes, ie shared responsibility.[3] The drive to achieve cost benefit efficiency or effectiveness in establishing and providing services is a principal reason for the development of these closer agency working relationships.

In order to realise the opportunity of achieving the intended benefits from these closer working relationships, it is essential that the agencies involved clearly understand their respective responsibilities and accountabilities. It would also be expected that the quality of cooperation between the agencies in discharging their respective obligations would be of a high order. Good public administrative practice requires that these matters be formalised between the agencies in a 'Memorandum of Understanding' or 'Service Level Agreement'. This is essential to avoid any misunderstanding concerning their respective obligations.

Finally, another area that serves to maintain public confidence in government operations, relates to the matter of regular independent oversight of operations. There can be systems and processes of government that present certain risks that require close management and regular monitoring to meet the public expectation of their proper functioning at all times. The implementation by agencies of effective independent assurance or audit in relation to these high risk systems and processes is an effective means of meeting this expectation.

1.3 Audit Mandate

The Audit review process for the purpose of this Report 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. 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 effective management, security, and control of computing systems and computing environments is essential to enable an agency to meet its operational objectives and financial accountability obligations. Effective management in these matters contributes to the ongoing integrity, continuity, and control of agency operations, and the protection of its information and assets. Conversely, inadequate management can lead to sub-optimal operational systems and the risk of error or loss of information and assets, resulting in unnecessary expense, or indeed, the incurring of potential liabilities.

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

1.4 Matters Examined by Audit

The three systems that are the subject of this Report were reviewed in relation to the following matters:

- Agency organisation structure, governing requirements for system operation, and roles and responsibilities of key personnel.

---

[3] Examples include, a government agency engaging with another agency to undertake a shared responsibility and outcome, or an agency with particular resources or expertise providing services to another agency.

- Specific security and control arrangements and measures, including:

  - security policies and procedures;
  - operating procedures for system and facilities;
  - access to system and information;
  - database and system implementation and support;
  - network support;
  - system maintenance.

- Business continuity arrangements, including system recovery arrangements.

In reviewing these three systems regard was given to any formalised arrangements covering system operation and maintenance between one government agency and another government agency or external service provider. Attention was also directed to the agency's conformance with the requirements set out in the ISMF document.

Sections 3 and 4 of this Report provide detailed comment in respect of each of the three system reviews undertaken. This includes background information concerning the review and relevant details of Audit communications outlining review findings to agency management. The responses of those agencies to the Audit communications is also included.

The following section of this Report discusses the key Audit findings. These key findings are discussed having regard to the important issues of principle and practice that have been referred to above.

2. KEY AUDIT FINDINGS

2.1 Obligation of Agencies to Comply with the Law

Within Government there are certain agencies whose operations are required to comply with specific statutory arrangements. It is important that these agencies comply with those arrangements.

It is also important that where the requirements of legislation may not be absolutely clear that expert legal advice should be sought to enable proper procedures to be implemented that provide for compliance with the matters that are mandated by the legislature.

Governing requirements with respect to the establishment and operation of the SACREDD DNA database system are contained in the *Criminal Law (Forensic Procedures) Act 1998.* They relate to, inter alia, forensic procedures generally, how forensic material is to be dealt with (including destruction), the DNA database system, (including the establishment and use of various indexes) removal of information, allowed access and use of information, and maintenance of confidentiality of information.

Certain issues relating to compliance with legislation and the need for legal clarification were identified in respect of the audit of the management and control of the SACREDD DNA database system. The management and control of this system is under the *Criminal Law (Forensic Procedures) Act 1998,* vested in the Commissioner of Police. The Commissioner has, in turn, delegated to the Director, Forensic Science SA to carry out certain of the responsibilities of the Commissioner under the abovementioned Act. The Commissioner has also entered into a Memorandum of Understanding with the Director, Forensic Science SA regarding several matters associated with the administration of matters that arise under the abovementioned Act.

In respect of the operation of the SACREDD DNA database system, two of the matters that were identified in the course of the audit relate to the creation of additional systems/records that contain DNA data, and destruction and removal of DNA information from the DNA database and associated records.

2.1.1 Additional Systems/Records

The *Criminal Law (Forensic Procedures) Act 1998*, under which the SACREDD DNA system operates, envisages a single DNA database being maintained. However, the review found that there were other systems/records containing DNA related information that were also being maintained on the database. Audit considered that there was doubt that these systems/records may not be authorised under the Act. One such matter related to the recording of DNA profiles of Forensic Science SA staff members.

Advice was sought by Forensic Science SA from the Crown Solicitor's Office on the matter of maintenance of other systems/records, including Forensic Science SA staff DNA profiles. In February 2005 the Crown Solicitor's Office advised that the maintenance of other systems/records to assist with the administration and maintenance of the DNA database was not in conflict with the legislation. That advice, in specific reference to Forensic Science SA staff DNA profiles, was based on the understanding of the Crown Solicitor's Office that those profiles were not placed on the database system to form any index on the database. Whilst this information may not 'form any index on the database' it is not information that is specifically authorised under the legislation to be included on the database. As noted above, the Audit review found that the information has been included on the database.

Whilst information on staff DNA profiles is acknowledged as a critical component of the system quality assurance process in the elimination of any potential contamination from Forensic Science SA staff, it is nonetheless, in my opinion, not contemplated in the existing legislative framework for inclusion on the DNA database.

As the storage of such information is not recognised in the legislation, Audit requested the Police Department and Forensic Science SA to seek further consideration of the matter by the Crown Solicitor's Office to ensure that the maintenance of the Forensic Science SA staff DNA profiles on the DNA database is permitted by the legislation.

The Crown Solicitor in early September 2005, provided advice indicating that the maintenance of Forensic Science SA staff DNA profiles was, in his opinion, permitted by the legislation. The advice also indicated that it would be possible to enact a Regulation under the Act establishing a specific index comprising DNA profiles of Forensic Science SA staff. In my opinion, it is important that there be no ambiguity regarding the operation of the DNA database and the information that can be lawfully held on it. Where the legislation is silent on a particular matter that is of importance, the responsible course of action should be to legislatively clarify the position.

The Crown Solicitor's advice supported the enactment of such a Regulation. Firstly, that Regulation would have the effect of specifically defining the index use for the purpose of identification of contamination and for other related purposes. Secondly, it would also have the effect of defining restrictions placed on the access to that information and to provide for the maintenance of its confidentiality.

In my opinion, the enactment of a Regulation with subsequent recognition of the Forensic Science SA staff DNA profile index under the legislation would formally recognise and regulate the use of the index and its information for this purpose. It is understood that the Police Department and Forensic Science SA will recommend to Government the enacting of a Regulation. In my opinion, this should be undertaken as a matter of priority.

2.1.2 Destruction and Removal of DNA Information

The *Criminal Law (Forensic Procedures) Act 1998* includes certain provisions[4] under which forensic material must be destroyed and DNA information removed from the DNA database.

For example, where a crime suspect is not subsequently convicted, the *Criminal Law (Forensic Procedures) Act 1998,* requires destruction of the forensic material (section 44C) and removal of DNA information. The destruction is deemed to occur if it is not possible to identify the person from whom the material was obtained or to whom the material relates.[5] This involves both the destruction of the material and the removal of information from the database, temporary files, back up media, and hard copy records.

Neither the Act nor the 'Memorandum of Understanding' established between the Commissioner of Police and the Director, Forensic Science SA, provide specific procedures for the destruction and removal requirements under the Act.[6]

4 *Criminal Law (Forensic Procedures) Act 1998,* sections 44A, B, C, D, and section 46C.

5 *Criminal Law (Forensic Procedures) Act 1998*, Part 1 – Preliminary, Interpretation section 3 (3)

6 It is important to comment here that the Audit review focus was on the SACREDD DNA database system. It therefore looked at, amongst other matters, the processes involving removal of information from the DNA database. It did not extend to an examination of the processes for the destruction of the physical forensic DNA material.

As early as 2003, Forensic Science SA had developed a series of procedures to remove data from the DNA database and destroy electronic and hard copy records as required by the Act and sought acceptance of those procedures by the Police Department. Although the procedures have been in operation, it was only in mid September 2005 that the destruction and removal procedures were formally accepted by the Police Department.

In May 2003, the Crown Solicitor's Office provided advice on the destruction of forensic material and removal of DNA information from the database. The advice noted that to satisfy the *Criminal Law (Forensic Procedures) Act 1998,* that is for destruction to be effective, it must not be possible subsequent to destruction and removal, to identify the person from whom the material was obtained or to whom the material relates. As such, the advice indicated that destruction and removal includes electronic records, hard copy documents and records, and backup media.

2.1.3 Non-Authorised Retention of DNA Information

The Audit review identified that there was not strict compliance in the destruction and removal of DNA information from all electronic and hard copy records, including temporary files and backup media. These matters were communicated to the Police Department and DAIS.

The Police Department and Forensic Science SA indicated that the destruction and removal of DNA information from electronic files and hard copy records was a manually resource intensive process. As such, there was a backlog in destruction and removal of DNA information.

It was further advised by the Department and Forensic Science SA that certain proposed system developments would facilitate this process. The system developments, however, would not be implemented until December 2005.

In relation to backup media, arrangements were in place to maintain copies of DNA information for an extended period of time. This is to enable the recovery of the DNA information in the event of unplanned adverse events affecting the DNA database and information availability. This represents good control practice for computer based systems. Nonetheless, the maintenance of backup copies containing DNA information for an extended period of time is not in strict compliance with the statutory requirements of the Act.

The importance of ensuring strict compliance with the Act in relation to the destruction and removal of DNA information from all electronic files and hardcopy records, including temporary files and backup media, was directly communicated to the Chief Executive, DAIS and the then Acting Commissioner of Police. That communication stressed the importance of implementing remedial action as a matter of urgency.

Shortly after informing the then Acting Commissioner of Police and the Chief Executive of DAIS, I received positive written advice confirming immediate implementation of action to effectively address the matters. That action included, commitment of resources to address the backlog of destruction and removal of DNA information from electronic and manual records, and a revised backup regime for the DNA database system. Audit was also advised that an enhanced internal audit process would be implemented to ensure the destruction and removal process are maintained in accordance with the Act.

2.1.4 Concluding Comment

The significance of the DNA database requires that the computer and related record keeping processes are undertaken in a manner that guarantees the integrity of DNA profile information, its recording, its confidentiality, and timely removal where required by legislation.

In my opinion, having regard to the public interest importance of this matter, any latent ambiguity regarding the establishment of a separate index for Forensic Science staff DNA profiles within the DNA database should be addressed by Regulation as a matter of priority.

2.2 Relationships Between Government Agencies for Effective Outcomes

In recent years, agencies of government have in some instances been required to work together for the purpose of undertaking a shared responsibility and/or response to achieving an effective outcome(s) in relation to a government initiative(s). This situation applies in relation to the SACREDD DNA database system which involves multi-agency involvement comprising the Police Department, DAIS and Forensic Science SA, and the Crown Solicitor's Office. EDS Pty Ltd also provides processing, storage and restoration services in relation to the system.

In order to achieve optimum 'connectedness' between the agencies and therefore effective outcomes, responsibilities and accountabilities of the agencies need to be clearly understood, and the quality of cooperation (including in matters of communication, responsiveness and decision-making) need to be of a high order. In some of these matters it is essential that the relationships should be formally documented detailing the responsibilities and obligations of the various parties.

The importance of the matter of effective relationships between agencies was highlighted in the 1999 'Report to the Premier by the Prudential Management Group on Matters Reflecting on Good and Proper Administration Arising from the Cramond Report'.[7]

During the review of the DNA database system, some matters were identified that relate to the effectiveness of relationships between agencies involved in the management and operation of that system.

2.2.1 Responsibility Relationship between the Police Department and Forensic Science SA

Under the *Criminal Law (Forensic Procedures) Act 1998*, the Commissioner of Police is responsible for the DNA database. Key aspects of its operations have been delegated to

---

7 The Cramond Report related to an inquiry into whether the then Premier misled Parliament in answering questions concerning a possible contract commitment to Motorola. One important matter arising from the inquiry, was that a significant lack of communication between two agencies of government (the former Economic Development Authority and the former Office of Information Technology), contributed to the uncertainty concerning the possible contract commitment to Motorola.

Following the Cramond Report, the Prudential Management Group was requested to report on any policy and management issues that needed to be addressed to improve the processes of government. The report of the Prudential Management Group found, in part, that:

> *The demonstrated lack of communication as from EDA to OIT, the outright failure by EDA to provide copies of relevant and material contracts to OIT, and to provide meaningful briefings to OIT, played a significant role in the chain of errors, misunderstandings, wrongful assumptions, misinformation and the eventual material and misleading statements to Parliament, all which events are clearly identified in the Cramond Report.*

In this context, it is also important to have regard to the report by D Clayton QC and R Stevens; 'Second Software Centre Inquiry; A Report into the Evidence Given to the First Software Centre Inquiry (The Cramond Inquiry)' the Director, Forensic Science SA, a separate branch within DAIS. There is also, as mentioned above, a Memorandum of Understanding (MOU) between the Commissioner and the Director associated with the operation of this relationship.

2.2.1.1 Memorandum of Understanding

The MOU outlines the agreed responsibilities of the Commissioner of Police and the Director, Forensic Science SA regarding the operation of the SACREDD DNA database system. The MOU includes provision for review on an annual basis by both the Commissioner and the Director, Forensic Science SA.

The audit identified matters that, in my opinion, indicated that the MOU required elaboration and/or clarification in certain respects. These matters included:

- the DNA database connectivity with other systems;
- specific responsibilities/accountabilities for the development and timely approval and implementation of fundamental policies and procedures for the DNA database system; and
- annual internal review of forensic procedures and database operations.

Consistent with the provision in the MOU for annual review, the Commissioner of Police and the Director, Forensic Science SA signed an updated MOU in April 2005. That MOU incorporated certain of the Audit observations that had been advised up to that time. Some other matters that have been the subject of recent Audit advice will require consideration in the next update of the MOU.

The matters already actioned include arrangements for regular annual audit of forensic procedures and operations of the DNA database. These matters ensure effective operation of the DNA database and strict compliance with legislative requirements at all times.

It is considered that the MOU should identify all areas where important policy and procedures are required. It should also clarify the specific responsibilities of the Police Department and Forensic Science SA for the development, approval and implementation of the policy and procedures.

2.2.1.2 Clarification of Delegations

A further matter identified by Audit with respect to delegations was the need to establish and document additional delegations for parties associated with the technical operations and support of the DNA database. This matter has now been addressed by the parties.

2.2.1.3 Policy and Procedures

Particular issues were noted where formalised procedures had not been endorsed in a timely and responsive manner, and where policy formulation that was under consideration for some time was still to be completed.

Destruction and Removal of DNA Information — An important matter relates to the destruction and removal of DNA information from the DNA database and associated records. As noted in the previous section of this Report, as early as 2003, Forensic Science SA had developed a series of procedures to remove data from the DNA database and destroy electronic and hard copy records as required by the Act. It had sought acceptance of those procedures by the Police Department. Although the procedures have been in operation, the Police Department had only recently advised Forensic SA of the formal endorsement of those procedures.

Policy on Known Deceased Persons DNA — A further matter concerns the development of a specific policy with regard to the inclusion of known deceased persons' DNA on the SACREDD DNA database. The *Criminal Law (Forensic Procedures) Act 1998* provides for the inclusion and use on the DNA database of known deceased persons' DNA.[8] It is recognised by the Police Department, that it would not be in the public interest for all known deceased persons DNA to be routinely placed on the DNA database.

The matter of policy development regarding known deceased persons DNA has been under consideration by the Police Department for some time. In March 2004, the Police Department identified the requirement for a policy to be developed between the Police Department and Forensic Science SA. At the time of preparation of this Report, the Police Department advised that a proposed legislative amendment to include known deceased persons DNA profiles on the DNA database was being addressed in a legislative submission currently being prepared. Any appropriate policy and procedure would be completed after legislative change.

Policy on Deceased Suspects Blood Samples — Another issue relates to the use of a deceased suspects blood sample.

Forensic Science SA performs post mortems on deceased persons at the direction of the Coroner. The post mortems include those relating to deaths arising from violence, unusual, or unknown causes. The blood samples which are taken during post mortems are kept by Forensic Science SA and are usually disposed of after a period of one year.

The Coroner does not, in the usual course, give any direction to Forensic Science SA in relation to disposal of these blood samples, once those samples are no longer required by the Coroner. There are no legal requirements, either statutory or at common law, that concern the return of the blood sample, any time limits upon retention of the sample, and no legal requirement that it must or must not be disposed.

A situation can arise where those blood samples may be required for DNA profiling by the Police Department associated with a criminal investigation involving a deceased suspect. This matter was considered, inter alia, by the Crown Solicitor in an advice of March 2003 to the Police Department in respect to the right of access and use of blood samples. The advice stated '… that quite clearly the Coroner cannot and would not be the appropriate person/body to authorise that police be permitted to have the sample and/or that it be DNA tested'. The Coroner's powers are limited to the issue of determining the cause of death and whether or not an inquest is necessary or desirable.

Furthermore, the view of the Crown Solicitor was that the legal status of a deceased suspects blood taken upon a lawfully authorised post mortem, is that there is no property in the blood sample (or if a court were to determine that there were, that it would rest with Forensic Science SA). In these circumstances, the Crown Solicitor considers that there is no law preventing Forensic Science SA from doing as it wishes with the sample (once the Coroner has determined that he no longer has an interest in the sample).

The advice noted that there are stringent procedures required under the *Criminal Law (Forensic Procedures) Act 1998* when obtaining and testing a DNA profile from a living suspect. It recommended that a policy be developed between the Police Department and Forensic Science SA regarding the criteria which should exist before the testing of deceased suspects' blood is undertaken at the request of the police for criminal

[8] The 'volunteers (unlimited purposes) index' provides for DNA profiles derived from deceased persons whose identity is known.

investigation purposes. Again, at the time of preparation of this Report the Police Department advised that a proposed legislative amendment regarding the use of deceased suspects blood samples was being addressed in a legislative submission currently being prepared.

To maintain an effective relationship, Forensic Science SA as a service-provider to the Police Department under delegated responsibilities, should be operating under clearly defined and approved documented policies and procedures. The Police Department has a responsibility to ensure that policies and procedures formulated by the Department, or by Forensic Science SA, are developed, approved and implemented in a timely and responsive manner.

2.2.1.4 Audit Arrangements

Another area under the MOU acknowledged the importance of the performance of annual internal audits of the operation of the DNA database system and Forensic Science SA procedures.

The MOU envisages internal audits to be initiated and undertaken by the Commissioner of Police and Forensic Science SA. The audits would cover both the DNA database system and forensic procedures under the responsibility of the Director, Forensic Science SA. In addition, the MOU recognises that Forensic Science SA, as an accredited member of the National Association of Testing Authorities (NATA), needs to comply with the quality management standards of that body. These standards require external audit by NATA every two years and an internal audit each year.

Notwithstanding the system having being in operation for a number of years, formalised administrative policy and procedural arrangements for annual internal audit reviews have not been in place. Key elements of such formalised arrangements would include agreed timeframes for audit conduct, scope of audit activity, method of conduct of the audit, and audit reporting and actioning responsibilities.

It is considered that the scope of audit activity should be extended beyond Forensic Science SA to also include the DNA related operations and activities of the Police Department. The consideration and implementation of such formalised arrangements would necessarily involve a coordinated approach to the audits and result in effectively meeting the requirements of both the Commissioner of Police and Forensic Science SA in relation to the audits.

The commitment to the significance of annual audits needs to be demonstrated by a formalised agreement between the Police Department and Forensic Science SA that clearly articulates arrangements and conditions for the performance of these audits. The nature of the audits to be applied with respect to a DNA database and forensic procedures is subject of further comment in section 2.4 of this Report.

2.2.2 The Crown Solicitor’s Office and the Police Solicitor’s Branch

The *Criminal Law (Forensic Procedures) Act 1998* provides for numerous legal requirements to be met in relation to such matters as:

- the collection and processing of forensic material;
- forensic analysis and inclusion of DNA information on the DNA database;
- subsequent matching and use of information for criminal investigation purposes;
- destruction of forensic material and removal of information from the DNA database.

These matters can be complex and involve certain activities to be carried out by both the police and forensic personnel.

In the conduct of the audit of the DNA database system, it was noted that the Police Department and Forensic Science SA have, over the period of system's operation, sought legal advice in respect of a number of matters. Those matters included aspects relating to:

- legislative requirements;
- DNA database system operation;
- Police Department and Forensic Science SA forensic procedural matters.

The legal advice, in the main, was obtained from the Crown Solicitor's Office. Audit noted that on occasion the Police Department had sought advice from its internal Solicitor's Branch. In these circumstances there is the potential for the advice received to be potentially in conflict. This is not a desirable situation having regard to the importance of the issues involved.

Issues requiring direction and clarification to ensure strict compliance with the legislation can arise at any time and need to be immediately responded to with high quality expert legal advice. In relation to this latter point Audit noted two particular occasions where advice sought and received had not been acted upon in a timely manner.[9]

Regarding the need for expert legal advice to the Commissioner of Police and the Director, Forensic Science SA to address complex issues,[10] it is considered that such advice should be sought from and provided by, a single source solicitor experienced in the area of forensic science.[11]

Audit's review of legal advice given in respect of the DNA system, found that the arrangements in operation have involved requests for advice from both the Crown Solicitor's Office and the internal Solicitor's Branch of the Police Department. Those requests have also been made by various personnel within both the Police Department and Forensic Science SA.

Given the significance of the DNA system in the administration of justice, it is Audit's view that agreed arrangements should be established by the Police Department and Forensic Science SA, to ensure legal advice is sought and applied in a consistent and effective manner. This could, in my opinion, be effectively achieved by developing expertise within a particular source, ie the Crown Solicitor's Office or the Police Solicitor's Branch. This is, of course, a matter for resolution by the parties.

2.2.3 Other Relationships

In relation to the DNA database system, DAIS Information Systems personnel and EDS (Australia) Pty Ltd provide technical support services and computing infrastructure for the system operation. Those support services include daily operational procedures, implementation of security access requirements, system processing and reporting, and backup and recovery functions.

---

9 See section 2.1.2 of this Report under 'Destruction and Removal of DNA Information' the matter of Crown Solicitor's advice of May 2003. See also earlier in this section of this Report under '*Policy and Procedures*' the matters of 'Policy on Known Deceased Persons DNA' and 'Policy on Deceased Suspects Blood Samples'.

10 See also the comments by the Royal Commissioner in the 'Report of the Kapunda Road Royal Commission' (2005) where he made similar observations regarding the need for expert legal advice on certain matters associated with that Report.

11 Recommendation from an Independent Preliminary Audit of the National Criminal Investigation DNA database (NCIDD) by the Commonwealth Ombudsman and the Federal Privacy Commission.

The important matter of clear and formally documented arrangements also needs to be established and communicated to these parties to ensure the legislative provisions, in particular for the DNA database security access, and the removal of DNA information, are fully understood and carried out. This is the responsibility of the Commissioner of Police and by the delegated authority, the Director, Forensic Science SA.

In this regard, the Commissioner and the Director, Forensic Science SA have recently addressed and documented arrangements for security access, and have endorsed revised arrangements for the backup and restoration of DNA information.

It is critical that these processes are operated under clearly defined and communicated procedures at all times and that those procedures evidence compliance with all requirements of the legislation for operation of the DNA database and the ISMF.

In my opinion, the Police Department and Forensic Science SA should conduct a regular review of the support services and the formalised arrangements provided to those parties.

2.2.4 Concluding Comment

The Audit review identified matters that, in my opinion, require consideration to enhance the effectiveness of the working relationships between the participating agencies. Those matters relate to the following:

- The clarity of role and responsibilities of the Police Department and Forensic Science SA need to be enhanced in a number of operational and procedural areas to evidence improved accountability and effectiveness of the working relationships between the parties. These areas relate to (i) legal, policy and procedural matters regarding operation of the DNA database system, and associated procedures of the Police Department and Forensic Science SA; (ii) technical support provided by external parties in relation to the DNA database system; and (iii) arrangements for quality assurance and audits of the system and associated Police Department and Forensic SA procedures.

- The need for the Police Department and Forensic Science SA to revisit the arrangements for the provision of legal advice to ensure efficiency and consistency on the matter of the interpretation of this complex legislation.

DAIS and Forensic Science SA and the Police Department have acknowledged the matters and advised specific actions completed or in progress to adequately address the issues.

At the time at the preparation of this Report, the Police Department advised that certain matters of a policy or procedural nature were being addressed through proposal for legislative change for consideration by the Government. This was to establish legal certainty with respect to those matters.

2.3 Government Agency Responsibility for Effective Security and Control over Computer Systems and Information

The Government, through its many agencies, uses computer information systems to process, transmit and store information critical to the performance of its key business operations including core governmental services and financial outcomes. Of necessity, there should exist the highest standards of security and control over these systems and the information held by them.

A significant number of issues were identified in relation to the three systems examined that presented risks of unauthorised access to the systems and information, and to the confidentiality, integrity and availability of the systems and information. In this respect, a number of the issues fell short of the ISMF minimum standards for security and control measures that are now mandated as government policy.

Some issues of particular note that were advised to agency management for attention in relation to the three systems reviewed are noted hereunder.

2.3.1 Security Classification of Information

Computer systems record, process and store information of varying degrees of importance and sensitivity. In accordance with the ISMF, government agencies are required to classify their information in terms of integrity, confidentiality, and availability, and undertake a risk assessment regarding its importance. Agencies must then implement adequate security controls over the information and the computer processing environment.

In the case of the SACREDD system information, it was necessary for the Police Department and Forensic Science SA to consult to agree certain classification aspects of that information.

The Police Department and Forensic Science SA have completed a risk assessment and agreed and finalised all information classification components for SACREDD data. (Refer section 3.4.4)

2.3.2 Documentation of Key System, Processes and Staff Responsibilities

Important aspects of management and staff responsibilities and processes associated with the key areas of a computer system and the processing environment in which it operates, requires clear formal documentation and communication to all relevant agency personnel. This facilitates the effective and controlled operation of the system and its operating environment.

In all three systems reviewed, there was inadequate maintenance of formal documentation relating, among other matters, to the controls over user access to the system and information, and inadequate controls and documentation regarding the procedures for implementing changes to the systems or information.

All agencies responded advising of actions being taken to address the deficiencies in formal documentation. (Refer sections 3.3.4, 3.4.4 and 4.4).

2.3.3 Access to Networks, Systems and Information

Databases and systems are required to be accessed to process, update, produce and report information. With respect to these matters it is essential that the security arrangements associated with access be adequate to meet the standards required under the ISMF.

In the case of the ULTRA Pathology system, while the computer room was subject to physical access control, the main entry into the building was not physically secured, nor were desktop computers which may contain sensitive information.

With respect to user access provision to the CaseMan and SACREDD systems, it was found that access rights granted to a number of users were not appropriately restricted having regard to their role and responsibilities. Further, weaknesses were identified in communication network access arrangements for the CaseMan and ULTRA Pathology systems, including those for users able to 'dial in' through networks to the CaseMan system.

Two of the systems reviewed, ie the SACREDD and ULTRA Pathology systems, were found to be operating on computers that were 'shared' with other systems and other databases. This presents the potential for access by a small number of highly privileged users (systems administrators) where systems and information may be inappropriately viewed and in certain circumstances may be changed. In addition, the computer 'production' and 'test' environments for the CaseMan system were not segregated on separate computers.

DAIS has taken remedial action to address the user access weaknesses and to also segregate the computer operating environments for the CaseMan and SACREDD systems. IMVS advised of changes made for the ULTRA Pathology system to have relevant actions of privileged users logged and reported to another Health Unit sharing use of the same computer. Action was also proposed to strengthen physical access security. (Refer sections 3.3.4, 3.4.4 and 4.4).

2.3.4 Logging and Monitoring of System and Information Access and Activity

The ability to detect events that represent unauthorised access and/or use of system functions or information is critical for the purpose of ensuring adequate security and control. Modern computer systems provide logging facilities to detect and record such events for review and monitoring by management and any internal audit review.

The appropriate logging and monitoring of user activity and key system events was not evident in each of the three systems reviewed. With the CaseMan system there was no logging or monitoring of database activity. In respect of the SACREDD system, whilst logging of some events did occur, there had not been a formal assessment by the agency to identify specific logging and monitoring requirements for the system and information. The required level of logging capability was not available with the current version of the ULTRA Pathology system, and there was inadequate monitoring of user access activity and the appropriateness of access rights granted to users.

DAIS advised it had completed a risk assessment of the SACREDD system and had taken action to improve monitoring of certain activity for both SACREDD and CaseMan. IMVS advised of proposals to address the provision of logging facilities in the next version of the ULTRA Pathology system. (Refer sections 3.3.4, 3.4.4 and 4.4).

2.3.5 Business and Systems Continuity

Agency management need to ensure continuity of their key database and system operations in the event of any disruptions caused by adverse events. This is generally achieved through an adequate business continuity management process, involving documented business continuity plans that are regularly maintained and tested.

Audit found that a documented and tested business continuity (including disaster recovery) plan had not been developed for the CaseMan system. In regard to the ULTRA Pathology system, while a disaster recovery plan had been prepared in draft form, the plan had not been finalised, tested and endorsed by management.

DAIS advised of the planned completion by mid 2006 of relevant disaster recovery and business continuity plans. IMVS indicated that existing resource limitations had delayed progress on this matter, and at the time of preparation of this Report, was seeking external resources to assist in this work. (Refer sections 3.3.4 and 4.4)

2.3.6 Agreements with External IT Service Providers

These days, many databases and systems of government agencies are developed and/or supported by external, information technology service providers. It is incumbent on agencies to ensure that formalised agreements are established with the service providers, and that the agreements clearly articulate the security and control requirements to apply to the database or system. Further, the agreement should address the matter of the development or support processes to be applied to the database or system.

The review revealed that an external service provider undertakes development and certain system administration tasks for the CaseMan system on behalf of Forensic Science SA. No contractual arrangement has been formalised between the two parties clearly defining the responsibilities for such matters as, expected service levels, cost details, and the treatment of intellectual property rights.

DAIS advised that the formalisation of a contract and service level agreement with the external service provider was expected to be completed by the end of 2005. (Refer section 3.3.4)

2.3.7 A Recent System Security/Confidentiality Failure in an Interstate Jurisdiction

A recent experience in the Victorian Government demonstrates the importance of ensuring that computer systems and computer processing environments of government are adequately managed and operated at all times within a secure and controlled manner.

The experience relates to the Victoria Police's Law Enforcement Assistance Program (LEAP) system. The system is used to record crime incidents and personal particulars and captures a range of information of interest to law enforcement. The information stored on LEAP is sensitive and personal.[12]

Due to issues associated with inappropriate release of confidential information and security and process around the LEAP database, the Victorian Government is to replace the system and is to establish a new body to manage LEAP and to oversee the implementation of a replacement system. The cost of the developments including the replacement system over three years is estimated at $50 million.

2.3.8 Concluding Comment

The audit findings from the three system reviews, and in a number of other reviews undertaken in 2004-05,[13] highlight shortcomings in agency systems meeting the Government's minimum security and control measures as defined in the ISMF. In general, the agency responses have demonstrated appropriate consideration of the review findings and advised of action being taken to address the issues.

---

[12] Report of Director, Police Integrity 'Investigation into Victoria Police's Management of the Law Enforcement Systems Program (LEAP)', March 2005. The report indicated that information on LEAP must be protected against unauthorised access by effective policy, procedures and appropriate technology.

[13] In Part B of the 2004-05 Annual Report of the Auditor-General specific comment is included in various agency reports covering findings arising from reviews of computer systems and computer processing environments.

As already noted, Chief Executives are responsible for security within their agencies. It is important that an ongoing review program is undertaken within each agency to ensure systems and related security and control measures meet the minimum standards. In cases where agencies have internal audit capability, the internal audit programs of those agencies should have some coverage devoted to the review of their significant computer systems and operations, including review of compliance with the Government's ISMF. This is especially important where systems contain information of a personal and sensitive nature. The public would rightly expect security and control to be of a high order as inadequacies in these matters have a tendency to undermine public confidence in the institutions of government.

2.4 Quality Assurance and Audit of DNA Database Operations and Forensic Procedures

The previous section of this Report presented summary findings of a security and control nature arising from the audits of the three systems that are the subject of this Report.

The commentary in this section relates to the SACREDD DNA database system. It has authoritatively been accepted as proper practice that DNA databases should operate under quality assurance standards and be subject to regular independent oversight to maintain public confidence in the integrity of those database systems.[14] The nature of the SACREDD DNA database system and its importance in the administration of the criminal justice system necessitates that the expectations regarding quality assurance standards be met at all times.

Section 2.2.1.4 of this Report[15] indicated that the MOU between the Commissioner of Police and the Director, Forensic Science SA recognises the important aspects of quality assurance standards and regular internal audits of the SACREDD DNA database system and Forensic Science SA procedures.

2.4.1 Quality Assurance Standards

Forensic Science SA is an accredited member of the National Association of Testing Authorities (NATA) and requires external audit by NATA every two years and an internal audit each year. NATA undertook an external audit in May 2004 and Forensic Science SA completed an internal audit in June 2005. The Forensic Science SA internal audit did not assess aspects of compliance with the *Criminal Law (Forensic Procedures) Act 1998*.

It should be noted that the Auditor-General's review was undertaken independently and without consideration of the NATA or Forensic Science SA reviews.

---

14 Speech by the Hon Justice Michael Kirby, '*DNA Evidence: Proceed with Care*', March 2000.

Congressional Testimony, Testimony of Dwight E Adams, Deputy Assistant Director, Laboratory Division, FBI, '*The FBI's DNA Program*', June 2001.

Submission to the Australian Law Commission and Australian Health Ethics Committee Joint Inquiry into '*Protection of Human Genetic Information*', December 2002 by the Office of the Victorian Privacy Commissioner.

Australian Law Reform Commission Report 96 '*Essentially Yours: The Protection of Human Genetic Information*', May 2003.

The Houston Chronicle '*More DPS Labs Flawed*', March 2004.

'*Independent Preliminary Audit of the National Criminal Investigation DNA Database (NCIDD)*' by the Commonwealth Ombudsman and the Federal Privacy Commissioner.

15 See section 2.2.1.4 of this Report under '*Audit Arrangements*'.

2.4.2 *Internal Audits*

As noted above, Forensic Science SA is required to undertake an internal audit annually. The Commissioner of Police, as the officer responsible for the operation of the DNA database, may also undertake an internal audit of the DNA database and Forensic Science SA procedures. This audit activity is recognised under the MOU between the Commissioner and the Director, Forensic Science SA. The Police Department recently advised Audit that it has initiated action with Forensic Science SA with respect to the conduct of annual audits.

In my opinion, the audit to be initiated by the Commissioner of Police should have, as an element associated with its conduct, the matter of 'independence'. It should also necessarily involve persons with appropriate forensic science experience. This will ensure that the audit is consistent with the generally accepted authoritative view and practice for oversight of DNA database systems.

2.4.3 *Concluding Comment*

In my opinion, the number of issues arising from the audit review of the SACREDD DNA database system has indicated the importance of a combination of regular internal audit and expert external independent review.

The commitment to annual audits needs to be demonstrated by a formalised agreement between the Commissioner of Police and the Director, Forensic Science SA that clearly articulates the arrangements and conditions for the performance of annual internal audits.

This matter is currently being addressed by the Police Department and Forensic Science SA. The Police Department and Forensic Science SA have advised of the formalisation of comprehensive arrangements for both internal and external audits and is in the progress of implementing audits under those arrangements.

3. THE DEPARTMENT FOR ADMINISTRATIVE AND INFORMATION SERVICES

3.1 Background

The responsibilities of the Department for Administrative and Information Services (DAIS) include the development and implementation of policies and service delivery strategies across Government, and the delivery of a broad range of functions and services on behalf of the Government. These include:

- project risk management, building asset management, procurement and contract services;
- capital building works and major projects delivery;
- information technology policy, support and management services;
- fleet management;
- land valuation, survey and registration;
- workplace registration and regulation;
- industrial relations services;
- administration and assistance to the recreation, sport and racing industries;
- public sector workforce relations.

3.2 Forensic Services

A major DAIS service responsibility is in the area of forensic science. The Forensic Science SA Branch of DAIS provides independent pathology and scientific support services to the justice system and the South Australian community. DAIS operates two important systems to meet its forensic requirements, ie the CaseMan system and the SACREDD DNA system.

DAIS, in conjunction with the Police Department, is directly involved in the administration of the *Criminal Law (Forensic Procedures) Act 1998.*

Forensic Science SA is located in the Forensic Science Centre which houses a DNA laboratory and analytical equipment.

3.3 The CaseMan System

3.3.1 System Purpose and Functionality

The CaseMan system provides forensic Case Management functionality to Forensic Science SA. It is used, amongst other tasks, to ensure the chain of access to evidence is correctly recorded for criminal proceedings. CaseMan was developed and is supported by a private sector IT service provider.

It is relevant to note that the legal integrity of the forensic process principally rests with the hard copy case file. Nevertheless, there is sensitivity and risk associated with access to confidential Forensic Science information and the identities of persons held within CaseMan.

Approximately 80 laboratory personnel who are located in the Forensic Science Centre use the CaseMan system.

The CaseMan system operates on a computer in the basement of the Forensic Science Centre building with links to the production database housed at DAIS, Wakefield House. The system has 'Development' and 'Acceptance Test' environments.[16] DAIS manage the Acceptance Test environment and EDS manage the Development environment.

3.3.2 Why Issues Associated with CaseMan are of Public Interest Importance

Forensic procedures are undertaken by Forensic Science SA with details relating to procedures recorded for case management purposes in the CaseMan system. Details processed and recorded include highly confidential information relating to the nature of the forensic procedures pertaining to the individual cases, including the recording of the identities of persons. As mentioned above, the system, amongst other tasks, is used to ensure that the chain of access to evidence is correctly recorded for criminal proceedings.

The nature of this system, involving case recording of confidential and sensitive information, and the potential legal and other risks associated with the use and custody of that information, ie for criminal justice purposes, make it critical that the security and integrity arrangements in relation to the system are of a high standard. This requires compliance with the Government mandated ISMF.

3.3.3 Issues that have been Identified in the Course of the Audit

In 2004, Audit reviewed the CaseMan system and its computer processing environment. The audit findings were communicated to DAIS/Forensic Science SA in August 2004 and a response was provided in August 2004. That response advised of remedial actions to be completed with timeframes varying from one month to twelve months.

In February 2005, Audit sought an update from the Department on the status of remedial action with respect to one particular matter namely, the planned finalisation of contract documentation with the CaseMan system provider. A response was received by Audit in March 2005.

In June 2005, Audit completed a follow up review of certain actions taken regarding the matters identified in 2004. The review findings were formally communicated to DAIS/Forensic Science SA in August 2005 and a response received in September 2005.

The table in section 3.3.4 provides a summary of the specific areas subject to Audit's review, initial Audit reported findings, agency initial response, further Audit reported findings, and subsequent agency response.

---

16 The Development and Acceptance Test environments allow for changes to be made and tested independently of the live system, before being put into operation in the live system and the production database.

3.3.4 *Audit Communication Matrix — Audit Findings and Agency Responses*

Auditable Review Area	Initial Audit Reported Findings	Agency Response	Subsequent Audit Further Reported Findings	Agency Response
Contractual Documentation with CaseMan System Provider	The review found a lack of formalised contractual documentation of arrangements with the CaseMan Support Vendor. There was also the need to take into consideration any intellectual property matters in contractual documentation.	A formal contract would be developed with the support vendor, and would include consideration of ownership of intellectual property rights, as well as the development and maintenance of contractual obligations and costs.	Forensic Science SA had developed a draft contract with the support vendor. Audit recommended that Forensic Science SA progress the finalisation of the contract with the support vendor.	Formalisation of the contract with the support vendor had been delayed whilst DAIS had under consideration joint contract support arrangements for both Forensic Science SA and State Fleet business applications. DAIS subsequently advised that it would finalise a contract with the support vendor specifically for the CaseMan system. It is anticipated this would be completed by the end of 2005. Forensic Science SA considered the need to retain intellectual property rights as against certain benefits of development work being received from the support vendor. Continuation of these benefits are fundamental to the agreement with the support vendor.

Auditable Review Area	Initial Audit Reported Findings	Agency Response	Subsequent Audit Further Reported Findings	Agency Response
Security and Control	The SA Government Information Security Management Framework (ISMF) provides minimum information technology security standards and guidelines for implementation by agencies. The review found areas in the security management arrangements that did not fully comply with the policies, standards, guidelines and control mechanisms set out in the ISMF document.			
Security Policy and Procedures	The review found a lack of formal documentation of:			
	• Specific security requirements for Forensic Science SA;	Forensic Science SA advised that a review of DAIS policies would be undertaken and if risks were identified, specific policies for Forensic Science SA would be developed.	Documentation had not been finalised, including the development of specific Forensic Science SA information security policies.	In a general context, Forensic Science SA had conducted a risk assessment of its information systems against the ISMF. Key policies and procedures would be developed from this assessment and then documented. The estimated timeframe for completion would be within the next twelve months.
	• Details of the levels of application and network access granted to each user/group, review of user access rights and logging and monitoring.	Specific policies and procedures relating to access would be put in place and would correlate to Forensic Science SA operational roles. All CaseMan user documentation would be updated.	Documentation of levels of access granted to each user group, including the functionality/privileges available to each profile and log file review arrangements had not been finalised.	A detailed document had been developed and mapped against CaseMan roles to appropriate user levels and to individuals. Certain other documentation would be completed by the third quarter 2006.

Auditable Review Area	Initial Audit Reported Findings	Agency Response	Subsequent Audit Further Reported Findings	Agency Response
System Change Procedures	Lack of formal documentation of: • Recording or requesting changes to the CaseMan application to the support vendor; Testing requirements, pre-approval of migration of changes to production, and user sign-off or acceptance.	A comprehensive change request procedure had been developed and was in the process of implementation. The change request procedure also addressed approval, testing and migration to production, and changes to CaseMan data.	The change request procedure had been implemented.	
System and Information Access	The review found: • Inappropriate high-level access rights to the CaseMan database given to a significant number of staff;	High level user database access arrangements would be reviewed. A process to review staff access levels on an annual basis would be established.	Forensic Science SA had requested EDS to review and reduce the number of legacy database administrator accounts. Audit recommended Forensic Science SA continue the review of database administrator users.	Re-assessment of currently approved administrator user accounts would be conducted at the annual IT Security Review which would take place in June 2006, and annually thereafter.
	• Network weaknesses, including potential for any SA government 'dial up' user to make unauthorised access to the CaseMan database;	Forensic Science SA advised that network and application security would be tightened significantly, including access to CaseMan for external users. Forensic Science SA would also approach EDS in order to implement remote network activity logging.	Remote network activity logging was not possible under the current network infrastructure.	

Auditable Review Area	Initial Audit Reported Findings	Agency Response	Subsequent Audit Further Reported Findings	Agency Response
System and Information Access (Continued)	• Insufficient levels of access rights and cases of poor construction and use of passwords.	The access rights arrangements would be addressed as part of a new change management process. Tighter password and access controls would be implemented.	The review of profile access and Forensic Science SA requirements for this access had not been completed. Forensic Science SA continue mapping of operational roles and provide greater levels of profiles, to better match the roles assigned.	A review of access had been undertaken and mapped against, roles, access, and individuals assigned. A Forensic Science SA Information Security Review would occur annually.
Data Change Control	The audit identified no formal data change request forms existed for changes to sensitive CaseMan data.	A new Forensic Science SA change request procedure defining individual level of authority within Forensic Science SA and approval for the change had been developed. The procedure covered changes to CaseMan data and would be documented and implemented.	A CaseMan change process had been developed. Audit recommended Forensic Science SA re-emphasis the importance of completeness of all aspects of the change forms.	A Forensic Science SA internal audit completed in June 2005 indicated that most forms were filled in correctly. A communication had been sent to all staff in August 2005 reminding them of the requirements to fill in change request forms completely.
Event Logging and Review	The review identified: • no logging of database activity or monitoring of such activity;	Full logging of all relevant edits to CaseMan would be made, and these would be audited and reconciled against change request documentation.	Audit trails had been enabled within the CaseMan database for all changes to data. Logs track all changes whether made at application or database level. Forensic Science SA intend to perform periodic reviews of the database logs. Audit recommended Forensic Science SA assess whether there were any particular events/ trends that should be reviewed on a frequent basis, and where possible, extract such events for weekly review.	The annual Forensic Science SA internal audit currently make use of change request documentation and CaseMan logs in order to reconcile requests for critical data edit against edits conducted, and searches for unauthorised edits to critical data. This reconciliation would be further assessed at the next annual IT Security Review which would take place in June 2006, and annually thereafter.

Auditable Review Area	Initial Audit Reported Findings	Agency Response	Subsequent Audit Further Reported Findings	Agency Response
Event Logging and Review (Continued)	• While additions and changes to CaseMan data are logged, enquiry access to CaseMan data is not.	Forensic Science SA advised that logging of all enquiries was not warranted until a move was made to full electronic record keeping.	Audit recommended that Forensic Science SA document their assessment relating to enquiry logging as part of the ISMF risk assessment and keep the matter under review.	The need for such logging would be reassessed at the annual IT Security Review to be held in June 2006.
CaseMan Computing Environments	The CaseMan application production and development computer environments were not segregated.	Forensic Science SA indicated the environments would be segregated.	Forensic Science SA were in process of segregating the development and production environments in conjunction with EDS. Audit recommended that Forensic Science SA continue with the planned segregation of the development and production environments.	Forensic Science SA is moving towards segregation of production and development environments. This was envisaged to be completed by late 2005.
System Maintenance	Weaknesses were identified in the CaseMan and network server maintenance by EDS.	Forensic Science SA had contacted DAIS IS to ascertain from EDS details of system 'patch' (security updates) discrepancies associated with maintenance on the computer operating system and to address the matter.	Forensic Science SA had communicated with EDS. Further weaknesses were identified relating to critical security updates on the computer operating system environment which had yet to be installed. Audit recommended that Forensic Science SA pursue the matter with EDS.	Appropriate patches were installed in August 2005.
Business Continuity	Whilst controls over the backup processes appeared adequate, Forensic Science SA had not developed a specific documented and tested Disaster Recovery Plan for the CaseMan system.	A business continuity plan (BCP), and disaster recovery plan (DRP) were under development with DAIS anticipating completion in the next 12 months.	Forensic Science SA were in the process of creating a Forensic Science SA wide DRP. Audit recommended that Forensic Science SA continue with the development of the business continuity and disaster recovery plan.	Disaster recovery and business continuity plans were progressing. Estimated completion is mid 2006.

3.3.5 Concluding Comment

The main issues arising from the audit related to matters of contractual arrangements with the external system support provider, security and control weaknesses associated with formalisation of policy and procedure and computing system configuration and maintenance. There was also the matter of the business plan arrangements for ongoing operation of the system that require to be addressed.

The Audit Communication Matrix above, reveals that DAIS and Forensic Science SA have responded with planned positive action to addressed the matters that have been raised by Audit. Remedial action has been taken or target dates have been set for completion of planned remedial measures. Formalisation of contract arrangements with the system support vendor are in progress, action has been taken or is in progress to improve policy and procedure documentation covering a number of areas, and the development of disaster recovery and business continuity plans were in progress.

The comprehensive nature of the responses that have been received from DAIS and Forensic Science SA to all the audit issues including advice of target completion dates, indicates positive commitment by the agencies to improve the management control exercised over the CaseMan system and to align with the standards of the ISMF.

3.4 The SACREDD System

3.4.1 System Purpose and Functionality

The South Australian Criminal Reference and Evidence DNA database (SACREDD) system is primarily used for the searching and matching of nominated DNA profiles as determined by the *Criminal Law (Forensic Procedures) Act 1998* and their automated reporting to the DNA Management Section of the Police Department.

The DNA database system is operated by Forensic Science SA, under delegations and a Memorandum of Understanding with the South Australian Commissioner of Police. The *Criminal Law (Forensic Procedures) Act 1998* is intended to strike a balance between individual civil liberties, (eg personal privacy, the privilege against self incrimination and bodily integrity), and the public interest in effective investigation and prosecution of criminal offences.

The SACREDD system operates on a computer in the Forensic Science Centre with links to the production database housed at DAIS, Wakefield House. The system has 'Development' and 'Acceptance Test' environments. DAIS manage the Acceptance Test environment and EDS manage the Development environment.

3.4.2 Why Issues Associated with SACREDD are of Public Interest Importance

Similar to the CaseMan system, the SACREDD DNA database system processes and records highly confidential and sensitive information including the identities of persons.

The DNA database system is of critical importance in the administration of justice in this State. Its configuration, operation, and use of information on the database is governed by the legislative requirements of the *Criminal Law (Forensic Procedures) Act 1998*. The DNA forensic related information contained on the database is used for the investigation of criminal offences.

As the DNA database system involves the processing and storage of highly confidential and sensitive information, there are potential legal and other risks associated with the integrity, custody and proper use of the information for the purpose of the criminal justice system. In these circumstances, it is critical that the security and control arrangements in relation to the system are beyond reproach and are in compliance with the ISMF.

3.4.3 Issues that have been Identified in the Course of the Audit

In 2004, Audit reviewed the SACREDD system and its computer processing environment, including compliance of the DNA database system with the *Criminal Law (Forensic Procedures) Act 1998*. The Audit findings were communicated to DAIS/Forensic Science SA and the Police Department in November 2004 and responses were provided in December 2004. The responses advised of remedial actions to be completed with timeframes varying from one month to nine months.

In early 2005, Audit sought an update on the status of some remedial actions principally due to be completed within a six month timeframe, and to confirm or obtain additional information regarding advice from the Crown Solicitor's Office. Information was also sought regarding the matter of the current position relating to policy and procedure and details of an advised Legislative submission. Responses were provided in March 2005.

In June 2005, Audit completed a follow up review of certain action taken regarding the matters identified in 2004. The review findings were formally communicated to DAIS/Forensic Science SA and the Police Department in August 2005 and responses received in September 2005.

Further communication regarding clarification of some matters took place between Audit and DAIS/Forensic Science SA and the Police Department in September and October 2005.

The table in section 3.4.4 provides a summary of the areas subject to Audits review, initial Audit reported findings, agency initial response, further Audit reported findings, and subsequent agency response.

3.4.4 Audit Communication Matrix — Audit Findings and Agency Responses

Auditable Review Area	Initial Audit Reported Findings	Agency Response	Subsequent Audit Further Reported Findings	Agency Response
Inter Government Working Arrangements ***Responsibility Relationship between the Police Department and Forensic Science SA***	Under the *Criminal Law (Forensic Procedures) Act 1998*, the Commissioner of Police is responsible for the DNA database. Key aspects of its operations have been delegated to the Director, Forensic Science SA of DAIS. A Memorandum of Understanding (MOU) has also been signed between the parties. The MOU includes provision for review on an annual basis by the Police Department and Forensic Science SA.			
	The audit identified matters that indicated that the MOU required elaboration in certain respects. Some of the matters to be dealt with related to establishing and documenting additional delegations for parties associated with the technical operations and support of the DNA database; the DNA database connectivity	The Police Department and Forensic Science SA would meet to develop a new Memorandum of Understanding. This would be completed in 2005.	The Police Department and Forensic Science SA signed an updated MOU in April 2005. That MOU elaborated on certain of the audit observations at the time of its finalisation and signing. Some other matters that have been the subject of recent Audit clarification and actioning by the Police Department and Forensic Science SA would require consideration for elaboration in the next update of the MOU. In	The matters actioned included the provision of additional delegations and revised arrangements for annual audit of forensic procedures and operations of the DNA database The MOU includes a provision that allows it to be updated as and when required. Once policies were formulated regarding specific identified issues, the MOU would be updated. Formal weekly meetings are being held between the Police Department and Forensic Science SA to review policy and

Auditable Review Area	Initial Audit Reported Findings	Agency Response	Subsequent Audit Further Reported Findings	Agency Response
Responsibility Relationship between the Police Department and Forensic Science SA (continued)	with other systems; specific responsibilities/accountabilities for the development and timely approval and implementation of fundamental policies and procedures for the DNA database system; and annual internal review of forensic procedures and database operations.		this regard it was considered that the MOU should identify all areas where fundamental policy and procedures are required, and the specific responsibilities of the Police Department and Forensic Science SA for the development, approval and implementation of the policy and procedures. Audit recommended that the MOU be revisited on the finalisation of outstanding Police Department, DAIS (Forensic Science SA) formal policy and procedures, and in the context of any legislative changes to ensure it remains relevant.	procedure with respect to the Act and the DNA database system operation. Fundamental policy and procedures will be addressed and included in any revision of the MOU.
Policy Procedures	Neither the Act nor the MOU provide specific procedures for the destruction and removal requirements under the Act.			
Destruction and Removal	Particular issues were noted by Audit where formalised procedures had not been endorsed in a timely and responsive manner, and where policy formulation that was under consideration for some time was still to be completed.	DAIS advised that formal acceptance by the Commissioner of Police would be requested.	DAIS/Forensic Science SA obtain formal approval in regard to destruction and removal procedures from the Commissioner of Police.	Although the procedures have been in operation, the Police Department had only recently advised Forensic SA of the formal endorsement of the procedures.

Auditable Review Area	Initial Audit Reported Findings	Agency Response	Subsequent Audit Further Reported Findings	Agency Response
Destruction and Removal (continued)	As early as 2003, Forensic Science SA had developed a series of procedures to remove data from the DNA database and destroy electronic and hard copy records as required by the Act and sought acceptance of those procedures by the Police Department.			
	Destruction and removal also includes backup media and controlled restoration.	Forensic Science SA would develop procedures for authorisation of data restoration and provide it to DAIS.	That Forensic Science SA ensure that the authorisation process and specific restrictions regarding the restoration of SACREDD data from backup media are formally documented and communicated to DAIS.	Backup and restoration procedures for the DNA database had been endorsed and implemented.
Known Deceased Persons DNA			Another matter concerned the need for development of a specific policy with regard to the inclusion of known deceased persons DNA on the SACREDD DNA database.	
			The matter of policy development regarding known deceased persons DNA had been under consideration by the Police Department for some time. In March 2004, the Police	Audit was recently advised that proposed legislative amendment to include known deceased persons DNA profiles on the DNA database was being addressed in a legislative submission currently being prepared by the Police Department.

Auditable Review Area	Initial Audit Reported Findings	Agency Response	Subsequent Audit Further Reported Findings	Agency Response
			Department identified the requirement for a policy to be developed between the Police Department and Forensic Science SA.	
			Finalisation of a policy had not been completed.	Policy and procedure would be completed after legislative change.
Deceased Suspects Blood Samples			An issue that was raised relates to the use of a deceased suspects blood sample. Forensic Science SA performs post mortems on deceased persons at the direction of the Coroner. The post mortems includes those relating to deaths arising from violence, unusual, or unknown causes There are no legal requirements, either statutory or at common law, that concern the return of the blood sample, any time limits upon retention of the sample and no legal requirement that it must or must not be disposed. The position can arise where those blood samples may be required for DNA profiling by the Police Department associated with a criminal investigation involving a deceased suspect.	
			The Crown Solicitor in an advice of March 2003 to the Police Department noted that there are stringent procedures required under the *Criminal Law (Forensic Procedures) Act 1998* when obtaining and testing a DNA profile from a living suspect. It recommended	Audit was recently advised that a proposed legislative amendment regarding the use of deceased suspects blood samples was being addressed in a legislative submission currently being prepared by the Police Department.

Auditable Review Area	Initial Audit Reported Findings	Agency Response	Subsequent Audit Further Reported Findings	Agency Response
Deceased Suspects Blood Samples (continued)			that a policy be developed between the Police Department and Forensic Science SA regarding the criteria which should exist before the testing of deceased suspects blood is undertaken at the request of the police for criminal investigation purposes.	
Audit Arrangements	Another important area under the MOU acknowledged the significance of the performance of annual audit of the DNA operation and Forensic Science SA procedures.			
	The MOU envisages internal audits to be initiated and undertaken by the Commissioner of Police and Forensic Science SA. The audits to cover both the DNA database system and forensic procedures under the responsibility of the Director, Forensic Science SA. In addition, the MOU recognises that Forensic Science SA as an accredited member of the National Association of Testing Authorities (NATA), needs to	The Police Department has recently initiated action with Forensic Science SA with respect to the conduct of an annual audit.	The commitment to the significance of an annual audit needs to be demonstrated by a formalised document agreed between the Police Department and Forensic Science SA that clearly articulates the arrangements and conditions for the performance of annual internal audits. Audit further considered that key elements of such formalised arrangements would include agreed timeframes for audit	The Police Department and Forensic Science SA are implementing enhanced internal and external audit arrangements to operate from 2005. The enhanced arrangements will cover legislative compliance, DNA database system operations, associated Forensic Science SA and Police Department policy and procedures, and quality assurance requirements. Further, the annual quality systems internal audit will also specifically address the destruction process.

Auditable Review Area	Initial Audit Reported Findings	Agency Response	Subsequent Audit Further Reported Findings	Agency Response
Audit Arrangements (continued)	comply with the quality management standards of that body. These standards require external audit by NATA every two years and an internal audit each year. Notwithstanding the system having being in operation for many years, formalised administrative policy and procedural arrangements for annual internal audit reviews have not been in place.		conduct, scope of audit activity, method of conduct of the audit, audit reporting and actioning responsibilities, and also include the DNA related operations and activities of the Police Department. The consideration and implementation of such formalised arrangements would necessarily involve a coordinated approach.	
Expert Legal Advice			It was noted that the Police Department and Forensic Science SA have over the period of system operation, sought legal advice in respect of a number of matters, including aspects relating to legislative requirements, DNA database system operation, and Police Department and Forensic Science SA forensic procedural matters. Audit's review of legal advice given in respect of the DNA system, found that the arrangements in operation have involved requests for advice from both the Crown Solicitor's Office and the internal Solicitor's Branch	

Auditable Review Area	Initial Audit Reported Findings	Agency Response	Subsequent Audit Further Reported Findings	Agency Response
Expert Legal Advice (continued)			of the Police Department. Those requests have also been made by various personnel within both the Police Department and Forensic Science SA. On two particular occasions advice sought and received had not been acted upon in a timely manner.	
			Regarding the need for legal advice to address complex issues to ensure strict compliance with the legislation, it is considered that such advice should be sought from and provided by, a single source solicitor experienced in the area of forensic science. Those arrangements need to determine the appointed single source solicitor, and address formal protocols for instructing and requesting of the advice, and subsequent communication and actioning of the advice within the Police Department and Forensic Science SA. There is also a need to consider the role of the Commissioner of Police and Director, Forensic Science SA in respect of the arrangements.	The Police Department and Forensic Science SA agree that a single source provider of legal advice is desirable. Protocols will be developed by the Police Department and Forensic Science SA to ensure the need for advice is discussed and agreed and that an appropriate source is decided.

Auditable Review Area	Initial Audit Reported Findings	Agency Response	Subsequent Audit Further Reported Findings	Agency Response
Technical Support	DAIS IS personnel and EDS (Australia) Pty Ltd provide technical support services and computing infrastructure for the system operation, including daily operational procedures, implementation of security access, system processing and reporting, and backup and recovery functions. Audit conveyed that clear and formal documented arrangements need to be established and communicated to these parties to ensure the legislative provisions, in particular for the DNA database security access, and removal of DNA information are fully understood and carried out. This is the responsibility of the Police Department and Forensic Science SA.	The Police Department and Forensic Science SA have addressed the documented arrangements for security access and have endorsed revised arrangements for the backup and restoration of DNA information.	Revised arrangements have been implemented.	
Legal Arrangements and Compliance ***Additional Systems/ Records***	The Criminal Law (Forensic Procedures) Act 1998, under which the SACREDD DNA system operates, envisages a single DNA database being maintained.	Advice would be sought from the Crown Solicitor's Office on several matters raised by Audit.		

Auditable Review Area	Initial Audit Reported Findings	Agency Response	Subsequent Audit Further Reported Findings	Agency Response
Additional Systems/ Records (continued)	The review found that there were certain other systems/ records containing DNA related information that were being maintained. One notable matter related to the recording of DNA profiles of Forensic Science SA staff members. Audit's review found that DNA information concerning staff members from Forensic Science SA was stored on the DNA database system. Whilst the staff profile information does not form a specific index as defined in the legislation, Audit considered this may not be provided for under the Act. In raising this matter, Audit was aware of the critical need for this quality assurance process in the elimination of any potential contamination from Forensic Science SA staff.	In February 2005, the Crown Solicitor's Office advised Forensic Science SA that the maintenance of other systems/records to assist with the administration and maintenance of the DNA database would not be in conflict with the legislation.	As the storage of Forensic Science SA staff profile information is not recognised in the legislation, Audit requested the Police Department and Forensic Science SA to seek further consideration of the matter by the Crown Solicitor's Office.	Staff profile information is seen as a critical component of the system quality assurance process in the elimination of any potential contamination from Forensic Science SA staff. The Crown Solicitor in early September 2005, provided advice indicating that the maintenance of Forensic Science SA staff DNA profiles was permitted by the legislation. The advice indicated that it would be possible to enact a Regulation establishing a specific index comprising DNA profiles of Forensic Science SA staff. His advice included certain comments that strongly supported the enactment of such a regulation. Firstly, that regulation would have the effect of specifically defining the index use for the purpose of identification of contamination and for other related purposes. Secondly, it would also have the effect of defining restrictions placed on the access to that information and to provide for the maintenance of its confidentiality. A proposed legislative amendment for the enacting of a regulation is being addressed in a legislative submission being prepared by the Police Department. Audit considers the enactment of a regulation with subsequent recognition of the Forensic Science SA staff DNA profile index under the legislation would formally recognise and regulate the use of the index and its information.

Auditable Review Area	Initial Audit Reported Findings	Agency Response	Subsequent Audit Further Reported Findings	Agency Response
Destruction and Removal of DNA Information	The *Criminal Law (Forensic Procedures) Act 1998* includes certain provisions under which forensic material must be destroyed and DNA information removed from the DNA database.			
	Destruction involves both the destruction of the material and the removal of information from the DNA database and all temporary files.	A web-based front end was being developed that would facilitate the destruction and removal of certain temporary files. In the interim the temporary files would be destroyed manually.	The web-based front end was still under development and was not due for implementation until December 2005.	Forensic Science SA with DAIS IS was developing a web-based service to assist with destructions. The project is expected to be completed by the end of December 2005.
	Forensic Science SA had developed a series of procedures to remove data from the DNA database and destroy electronic and hard copy records as required by the Act. The Audit review identified that there was not strict compliance in the destruction and removal of DNA information from all electronic and hard copy records including those on back-up tapes.	Audit was advised in March 2005 that due to practical difficulties, the previously advised manual procedures would not be implemented.	There was not strict compliance in the destruction and removal of DNA information from all electronic and hard copy records, specifically with respect to temporary files and backup media.	The Police Department and Forensic Science SA indicated that the destruction and removal of DNA information from electronic files and hard copy records was a manually resource intensive process. As such, there was a backlog in destruction and removal of DNA information. Audit subsequently received positive written communications from the Police Department and Forensic Science SA advising immediate implementation of action to effectively address the matters. That action included, commitment of resources to address the backlog of destruction and removal of DNA information from electronic and manual records, and a revised backup regime for the DNA database system. It was also advised to Audit that an enhanced internal audit process would be implemented to ensure the destruction and removal process are maintained in accordance with the Act.

Auditable Review Area	Initial Audit Reported Findings	Agency Response	Subsequent Audit Further Reported Findings	Agency Response
Destruction and Removal of DNA Information (continued)		In March 2005, the Commissioner of Police provided Audit with a copy of a submission for legislative review requesting, amongst other matters, simplification of the destruction process.	A request for Legislative review had not yet been finalised.	A submission by the Police Department to change the Act in relation to destruction had been made to the Minister for Police in 2004, but concentrated on financial issues rather than the practical difficulties arising from attempting to comply with the Act. The Police Department was in the process of redrafting the legislative submission to also convey that there is difficulty in Forensic Science SA keeping up with destructions under current legislation. The submission of the draft is expected in the 1st quarter of 2006.
Security and Control	The SA Government Information Security Management Framework (ISMF) provides minimum information technology security standards and guidelines for implementation by agencies. The review found areas in the security management arrangements that did not fully comply with the policies, standards, guidelines and control mechanisms set out in the ISMF document.			

Auditable Review Area	Initial Audit Reported Findings	Agency Response	Subsequent Audit Further Reported Findings	Agency Response
Information Classification and Security	The information within the DNA database is of a critical and sensitive nature comprising personal forensic information.			
	The Police Department and Forensic Science SA needed to consult to agree over certain security classification aspects of DNA information. Audit believes consideration of public perception would suggest it should be given the highest confidentiality classification rating.	A risk assessment workshop would be undertaken in early 2005.	Proposed risk assessment against the Government ISMF requirements and the security and confidentiality classifications of SACREDD information, which were envisaged to be completed by February 2005, were still outstanding.	Risk assessment and classification of DNA data confidentiality, availability, and integrity had been completed. DAIS had been advised of the classifications and they were being used to devise architecture appropriate for the operation of SACREDD.
System and Information Access	The review found that certain administrative aspects of the database are outsourced to DAIS IS, EDS (Australia) Pty Ltd, and a external system developer. All these parties have various levels of access to the DNA Database. As the Act is silent in regard to any outsourcing, Audit sought confirmation of the acceptability of the practice.	The Police Department indicated it would seek Crown Solicitor's Office advice on the matter of access for administrative purpose. DAIS indicated it would review access six monthly including compliance with the Act with respect to third party service providers.	Forensic Science SA received advice from the Crown Solicitor's Office regarding third party access to SACREDD indicating DAIS IS/EDS and the other third party service providers access was allowable. The follow up review indicated that the assessment of user access rights had been addressed satisfactorily.	

Auditable Review Area	Initial Audit Reported Findings	Agency Response	Subsequent Audit Further Reported Findings	Agency Response
System and Information Access (continued)	The review revealed some weaknesses in security arrangements that required attention of management, including: • Informal processes for access to SACREDD; • User access higher than required; • No regular review of user access rights; • Users were not automatically logged out after a period of inactivity; • No formal assessment of specific logging and monitoring requirements. • Lack of formal documentation relating to user access and implementation of changes to the system or information.	A review of application security would be completed by mid 2005. Some key areas being addressed were: • Forensic Science SA to audit and review all changes to critical data; • User access to DNA database would be periodically reviewed; • Improvements to operating documented procedures, including documentation of procedures for change management.	The follow up review indicated that the matters raised by Audit had been satisfactorily addressed.	

Auditable Review Area	Initial Audit Reported Findings	Agency Response	Subsequent Audit Further Reported Findings	Agency Response
Integrity of System Reports	A range of reports and information from SACREDD is forwarded to the Police Department using 'pdf' documents that do not have security settings enabled. This allows the SACREDD data contained within the reports to be changed without the authorisation of Forensic Science SA. Audit considered security settings should be enabled on all key reports.	Security settings on reports relating to SACREDD data would be increased to enable print and read access only.	The follow up review indicated that the security over 'pdf' documents had been addressed.	
DNA Database Computing Environment	Weaknesses relating to database security controls, included: • the SACREDD DNA database was stored on a shared computer that contains a number of other databases. These databases share the same user access environment, making it possible for one privileged user to access other databases, including SACREDD.	A decision as to a appropriate environment for the SACREDD system would be made once a security classification review had been completed.	The review found that the SACREDD system computer environment was not segregated from other systems. Audit recommended that DAIS (Forensic Science SA) segregate the SACREDD system from the computer operating system that is shared with other systems/ databases.	A risk assessment had been completed and Forensic Science SA would proceed with the implementation of SACREDD on a stand-alone computer. Expected completion is the 3rd Quarter 2006.
	• The SACREDD database is located on the DAIS communications network rather than on an isolated network. This exposes the SACREDD database to a greater number of potential risks.	DAIS was in the process of performing a data risk classification assessment to identify the most appropriate course of action for the isolation of the network specifically for the SACREDD database.	The proposed data risk classification assessment for SACREDD had not been completed.	A risk assessment of the Forensic Science SA computer processing environment, including the DNA Database System, had been completed. The department will now proceed with the development of appropriate architecture for the SACREDD system in line with the risk assessment.

Auditable Review Area	Initial Audit Reported Findings	Agency Response	Subsequent Audit Further Reported Findings	Agency Response
DNA Database Computing Environment (continued)	Database security had not been enabled and passwords were not enforced.	Stronger password controls were being implemented.	The follow up review indicated that password controls had been addressed satisfactorily.	
Systems Operations Documentation	The review found that system documentation was not current including: • Some documentation reflected future plans rather than the current situation;	System documentation was being modified to only indicate current implementation.	SACREDD Systems documentation had been updated to only include current settings and implementation information. The follow up review indicated that the content of the SACREDD System Documentation had been addressed satisfactorily.	
	• No formal approval or notification process between Forensic Science SA and the Police Department for SACREDD changes initiated by Forensic Science SA.	Forensic Science SA would amend the MOU with the Police Department in order to include mechanisms for the Police Department's agreement to changes to the DNA database system.	A revised MOU was finalised in April 2005.	
	Forensic Science SA has not performed a risk analysis to identify their specific requirements for monitoring security events.	Forensic Science SA would log and review all manual edits of critical data in its 'case' information systems, including the DNA database system.		
	High reliance on one DAIS officer for technical support for the maintenance of SACREDD.	DAIS was taking steps to ensure that more than one individual is capable of supporting the DNA database system		

3.4.5 Concluding Comment

The audit review identified a number of important matters of principle and practice that were required to be addressed to meet the expected high standards of management and operational control for such a critical system as the SACREDD DNA database system. These matters related to compliance with governing legislation, effectiveness of the administrative arrangements between the agencies involved in the management of the DNA database system, and security and control issues associated with maintaining the integrity of the system and information including proper custody and use of system information.

As the issues were considered important in terms of public sector administrative principle and practice these issues are more fully discussed in section 2 of this Report.

The Audit Communication Matrix above, and more detailed discussion of a number of the audit issues in section 2 of this Report, shows that DAIS and Forensic Science SA and the Police Department have taken remedial action or are in the process of positively addressing the important issues. Illustrative of the positive action taken was the immediate engagement of additional resources by both DAIS and the Police Department to address the requirement of strict compliance with the *Criminal Law (Forensic Procedures) Act 1998* in the matter of addressing the backlog of destruction and removal of DNA information from the DNA database system and associated records.

The responses received from DAIS and Forensic Science SA and the Police Department, and the remedial action taken or in progress has been comprehensive in nature. This indicates positive commitment of the agencies to enhance management control over the SACREDD DNA database system and to meet legislative requirements and the standards of the ISMF.

4. THE INSTITUTE OF MEDICAL AND VETERINARY SCIENCE

4.1 Background

The Institute of Medical and Veterinary Science (IMVS) provides a range of diagnostic and consultative services in all branches of pathology for major public and private hospitals, medical practitioners and specialists, industry, and the general community. IMVS is also active in research programs and contributes to the education of students in various fields of medical science.[17]

The Institute has over eight hundred employees, and operates 4 metropolitan and 10 regional laboratories.

The IMVS computer systems that support its various functions are maintained by the Information Services Branch. This branch provides support for the clinical, administrative and research activities of the IMVS.

4.1.1 Pathology Services

The IMVS Pathology System supporting the clinical services function is the Centricity ULTRA Laboratory system (ULTRA). ULTRA is provided to the IMVS under a Whole of Health contract agreement with the Department of Health (previously Department of Human Services).

The ULTRA system operates on a computer in the IMVS building. The system has 'Development' and 'Acceptance Test' environments.[18] IMVS manage the Acceptance Test environment and EDS manage the Development environment.

4.1.2 The IMVS Pathology System Purpose and Functionality

The IMVS ULTRA Pathology System is the main laboratory management system for IMVS and has been in operation since 1998. ULTRA automates and integrates the laboratory processes, ie test initiation and results processing, and the management reporting and accounts receivable functions. The system processes approximately three million tests per annum and all laboratory test results are maintained on-line.

IMVS employees, across the main IMVS campus at Frome Road, Adelaide, the 4 metropolitan laboratories and 10 regional laboratories within South Australia, use the ULTRA system.

An Internet Web Browser facility provides for the viewing of pathology results to external Department of Health staff across metropolitan and country hospitals.

---

[17] An example of one of the different type of functions performed by IMVS can be found in the Molecular Pathology Unit of the Institute. This unit facilitates the diagnostic applications of nucleic acid-based technology and some of its major functions are to:

- Consolidate a range of DNA based tests for inherited genetic disorders;
- Develop DNA based tests for the mutations that predispose individuals to familial cancer;
- Establish a DNA sequencing service for the IMVS and Hanson Centre; and
- Engage in applied research into human genetic disease.

[18] Refer Footnote 15.

Additionally, ULTRA has been interfaced with the Institute's 'Homer' Financial System for the purpose of billing, and to the Department of Health OACIS Clinical Information System for use by Medical and Nursing staff of public and private hospitals. Billing claims for tests undertaken are submitted to the Health Insurance Commission (HIC) in line with preset Medical Benefit Schedule rates.

4.2 Why Issues Associated with ULTRA Pathology System are of Public Interest Importance

The IMVS has to date maintained a high level of integrity with respect to its pathology test results processing to the medical profession and to the community. Notwithstanding, the audit review has, in examining the ULTRA system operations against the standards that are now mandated for the public sector under the ISMF, identified certain risks associated with the maintenance of the integrity of critical and sensitive test result information and the ongoing availability of the system operation.

Requests for pathology testing and the results of those tests are highly confidential and are of major importance for patient diagnosis and resultant clinical management of those patients. Inaccurate, untimely delivery, or the unavailability of test result information, may lead to misdiagnosis and inappropriate patient management. The potential for prejudicial consequences in the event of error, inappropriate access to information or non-availability of results necessitates that there be a high degree of accuracy and control in the operation of the ULTRA system.

In this context, it is critical that the integrity of the ULTRA system operations and processes and the security arrangements regarding access to the system and information held on its database are fully compliant with mandated government policy requirements and applicable industry standards.

4.3 Issues that have been Identified in the Course of the Audit

In 2004, Audit reviewed the ULTRA system and its computer processing environment. The audit findings were communicated to the IMVS in July 2004 and a response was provided in September 2004. That response advised of remedial actions to be completed.

In June 2005, Audit completed a follow up review of action taken regarding the matters identified in 2004. The review findings were formally communicated to IMVS in July 2005 and a response received in September 2005.

The table in section 4.4 provides a summary of the specific areas subject to Audit's review, initial Audit reported findings, agency initial response, further Audit reported findings, and subsequent agency response.

4.4 Audit Communication Matrix — Audit Findings and Agency Responses

Auditable Review Area	Initial Audit Reported Findings	Agency Response	Subsequent Audit Further Reported Findings	Agency Response
Security and Control	The SA Government Information Security Management Framework (ISMF) provides minimum information technology security standards and guidelines for implementation by agencies.			
	The review found areas in the IMVS security management framework that did not fully comply with the policies, standards, guidelines and control mechanisms set out in the ISMF document.			
Policy and Procedures	Audit recommended that a gap analysis be undertaken and IMVS policies and procedures be reviewed.	A gap analysis and alignment of procedures would be undertaken over the next twelve months.		A process of engagement of resources to undertake this task had commenced.
	Further, the review revealed that a documented list of access approval delegates was not maintained.	Formal written procedures would be produced. A list of approval delegates had been implemented and would be reviewed bi-annually.	A new procedure had been created to ensure the authorised delegate lists are maintained and reviewed periodically.	

Auditable Review Area	Initial Audit Reported Findings	Agency Response	Subsequent Audit Further Reported Findings	Agency Response
System and Information Access	Areas that raised the potential for unauthorised access to the ULTRA system and database were:			
	• Certain IMVS privilege users had the ability to alter test result information. Additionally, another health unit shares the same computer and its privileged users have the ability to view and change data within the IMVS database.	The privilege user account is only used for managing the database and not for changing data. IMVS would create a log of any privilege user activity for subsequent review.	IMVS 'Work Request System' has been modified to ensure an alternate senior manager is required to approve work which requires the use of the privilege user feature to effect changes to data.	
	• Inadequate lockout controls over failed attempts to logon and access the system;	IMVS is to investigate if these features are available in the next version upgrade. If so it will be scheduled within the next 12 months.	A request had been sent to the system vendor, but a response had not been received. Audit recommended that the matter be followed up and IMVS consider available options for the locking of accounts and denying user access and for periodical reviews of the logs.	IMVS advised that the vendor planned to incorporate this in a new version of the system to be released in 2006.
	• No logging of failed logon attempts to access the ULTRA system;	In the interim IMVS has advised that successive unsuccessful login attempts are logged and communicated to the system administrator and reviewed daily.	Email communications being sent to the system administrator are investigated.	

Auditable Review Area	Initial Audit Reported Findings	Agency Response	Subsequent Audit Further Reported Findings	Agency Response
System and Information Access (continued)	• Inadequate monitoring on a periodic basis of approved system users, their activity and their respective access privileges;	IMVS would monitor active user accounts and access privileges for appropriateness bi-annually.	IMVS are performing reviews of inactive accounts, duplicate names and user identification, and expired passwords. The next review is scheduled for early 2006.	
	• Unsecure remote access to the IMVS network.	IMVS had now converted to a more secure access for all new services and will move to convert existing users to this service. Access is strictly limited to bona fide users.	The migration process for existing users is still in the process of being completed at the time of the review and was anticipated to be finalised in June 2005.	
System Change Procedures	The review identified inadequate segregation of duties in implementing system changes to the production environments.	IMVS would develop a form to detail changes and have an independent section manager review the changes.	The change management procedure has been modified to ensure that an alternate senior manager reviews all changes prior to their introduction into production. Satisfactory procedures have been defined to manage segregation of duties within the pathology system.	
Access to the Heritage Building Housing the Computing Facilities	Lack of security controls relating to physical access surrounding the IMVS heritage building and desktop computer facilities were identified.	IMVS to inform the owners of the building and liaise with them regarding options for improving the security of their building.	A formal letter has been provided to the RAH to investigate options. No response had been received to this request. Audit recommended that the matter be followed up for improving the physical security of the IMVS heritage building.	IMVS advised that discussions were being held with RAH regarding an upgrade of security.

Auditable Review Area	Initial Audit Reported Findings	Agency Response	Subsequent Audit Further Reported Findings	Agency Response
Environmental Controls over Computing Facilities	The review identified a lack of backup capability in the event of a fire.	Additional hand held fire extinguishers may be installed subject to professional advice.	Sprinklers and hand-held fire extinguishers have been installed within the facility.	
Business Continuity	The review found that the business continuity and disaster recovery plans were in draft format and had not been tested, reviewed and updated on a periodic basis.	IMVS would seek to progress finalisation of the business continuity and disaster recovery plans, including testing of the plans. The planned implementation of a new computer would also include a revision of the disaster recovery plan, documentation and testing.	Audit recommended that IMVS continue the business continuity and disaster recovery planning process to ensure appropriate prioritisation of system recovery tasks is aligned with business needs. A draft IMVS ICTS 'Pathology Computer System Upgrade' business case has been provided to IMVS executive to be finalised prior to the acquisition of the new hardware and preparation of the disaster recovery plan.	A process of engagement of resources to undertake this task had commenced.
	The current storage location of the plans may compromise the timely recovery of the ULTRA system in the event of a disaster.	IMVS would relocate the backup tapes and copy of the recovery plan off site in a RAH building.	The Backup tapes and disaster recovery plan have been relocated with all parties informed of the change.	

4.5 Concluding Comment

The main issues and risks identified during the audit process and reported to IMVS management related to certain weaknesses in the system and information access security arrangements and business planning continuity management.

In an overall context, weaknesses across these areas lower the standard of security that is expected to be in operation to prevent or detect unauthorised/unintended access to computing facilities and ULTRA system functionality and operation. In relation to business and system continuity planning, the business continuity and disaster recovery plans were in draft format and had not been tested, reviewed and updated on a periodic basis. The integral nature of the ULTRA system to IMVS meeting its significant service obligations to the medical profession and to the community, warrants up-to-date and tested plans. In the absence of such plans, there is a risk of unavailability of the system and test result information with consequential impact on patient health care.

As disclosed in the Audit Communication Matrix above, IMVS has considered and responded to the matters raised by Audit.

Whilst IMVS has implemented remedial action with respect to some issues there remain important matters that IMVS has advised its intention to address over a period of time. IMVS considered that certain matters were not easily or quickly rectifiable. For instance, some matters involve the need to change the system or be addressed in a future upgrade neither of which would be undertaken in the immediate future. Other matters required the engagement of resources to undertake the remedial tasks. Certain corrective action in this regard has recently commenced.

Under the current arrangements there remain potential risks that will require close management by IMVS. In recognition of the presence of those risks, there needs to be, where appropriate, interim measures, including closer and ongoing supervisory review or monitoring of relevant user and system activities.