The Auditor-General
Audit Report No.1 2002—03
Performance Audit

Information Technology at the Department of Health and Ageing

Department of Health and Ageing

Australian National Audit Office

© Commonwealth
of Australia 2002

ISSN 1036–7632

ISBN 0 642 80656 X

COPYRIGHT INFORMATION

The Manager,
Legislative Services,
AusInfo
GPO Box 1920
Canberra ACT 2601

or by email:
Cwealthcopyright@finance.gov.au

Australian National
Audit Office

Canberra ACT
18 July 2002

Dear Madam President
Dear Mr Speaker

The Australian National Audit Office has undertaken a performance audit in the Department of Health and Ageing in accordance with the authority contained in the *Auditor-General Act 1997.* I present this report of this audit, and the accompanying brochure, to the Parliament. The report is titled *Information Technology at the Department of Health and Ageing.*

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

Yours sincerely

Ian McPhee
Acting Auditor-General

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

AUDITING FOR AUSTRALIA

The Auditor-General is head of the Australian National Audit Office. The ANAO assists the Auditor-General to carry out his duties under the *Auditor-General Act 1997* to undertake performance audits and financial statement audits of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

Auditor-General reports are available from Government Info Shops. Recent titles are shown at the back of this report.

For further information contact:
The Publications Manager
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Telephone:	**(02) 6203 7505**
Fax:	**(02) 6203 7519**
Email:	**webmaster@anao.gov.au**

ANAO audit reports and information about the ANAO are available at our internet address:

http://www.anao.gov.au

Audit Team

Paul Nicoll
Eric Turner
Wayne Jones
Anne Martin
Jocelyn Ashford

Contents

Abbreviations/Glossary

ACCMIS	Aged and Community Care Management Information System. The Aged and Community Care Division developed ACCMIS as a central data repository from the Division’s operational computer systems, including SPARC
ANAO	Australian National Audit Office
BSB	Business Systems Branch at Health
CobiT	Control Objectives for Information and Related Technology
DMC	Departmental Management Committee
DSM	Department Security Manual
FMIS	Financial Management Information System
Health	Commonwealth Department of Health and Ageing
HIC	Health Insurance Commission
IBM-GSA	International Business Machines Global Services Australia
IPPC	Information Planning and Privacy Committee
ISACA	Information Systems Audit and Control Association
ISACF	Information Systems Audit and Control Foundation
IT	Information Technology
IT&T	Information Technology and Telecommunications
ITC	Information Technology Committee
OATSIH	Office for Aboriginal and Torres Strait Islander Health
ORAC	OATSIH Reporting Payments and Tracking System, a major application at Health for managing payments of funds to indigenous health services
PBS	Pharmaceutical Benefits Scheme
PIR	Post-Implementation Review
PSM	Protective Security Manual
SDLCM	System Development Life Cycle Methodology. The organisational arrangements and procedures involved in developing new computer applications or modifying existing systems or programs

SIME	Strategic Information Management Environment, a major application under development for the TGA to implement an information management framework, and to provide an electronic submission system for the listing or registering of therapeutic devices
SLA	Service Level Agreement
SPARC	System for Payments for Aged Residential Care, a major application at Health for managing payments of funds to residential aged care facilities
TECC	Technical Environment Change Control, used in conjunction with the TECC Committee
TGA	Therapeutic Goods Administration, a division of Health

Summary and Recommendations

Summary

Background

1. The Department of Health and Ageing *(Health)* is a major Commonwealth department with a diverse range of responsibilities which include promoting good health, ensuring all Australians have access to key health resources and promoting quality aged care services. For 2001–2002, Health's total appropriations were some $29 billion and its employment base was approximately 3500–3600 staff. A total of $14.7 billion of Health's appropriation was transferred to the Health Insurance Commission (HIC) for delivering government programs administered by the HIC on behalf of Health. A further $6.7 billion was paid to the state and territory governments as funding for public hospitals and related purposes under Australian Health Care Agreements.

2. The information technology (IT) environment at Heath is complex and the department relies considerably on IT to achieve its business objectives.

3. Health invests a significant amount of funds into IT, for example:

- the written down value of software developed and in operation at 30 June 2001 was $43 million, including $3.5 million of externally purchased software; and
- expenditure in 2000–01 for IT infrastructure services of $48 million, including a one-off transition cost payment of $19 million to the department's principal service provider.

4. Health holds large amounts of data and is responsible for the security and privacy of these data. Health currently maintains an extensive range of applications in order to support the diverse activities and programs managed within the department. These applications reflect both internally developed and purchased mainframe and client-server network applications.

5. Responsibility for IT at Health is devolved. Divisional heads own and are responsible for their divisions' IT systems. They are also responsible for their own IT strategic planning. The Business Systems Branch (BSB) provides programming and other IT support services to divisions, and it operates on a cost recovery basis for those services. Within a devolved environment, there is a need to ensure departmental consistency and integration of approach within an overarching system of control.

6. In June 2000, Health outsourced administrative and operational responsibility for its IT infrastructure services, including mainframe and server administration and management, to IBM Global Services Australia (IBM-GSA).

Although Health purchases IT infrastructure services, it retains responsibility for ensuring that effective controls are in operation.

7. On the basis of its status as a major department with a large IT investment, Health was selected by the ANAO for an audit of its management and operation of IT.

Audit objectives and approach

8. The overall objectives of the audit were to determine whether Health's management and operation of selected IT systems:

- meet industry better practice;
- meet quality and service delivery parameters set by Health and, if applicable, by the Government; and
- operate effectively, efficiently and economically.

9. The audit applied selected processes from CobiT (Control Objectives for Information and Related Technology), a framework of internationally accepted standards, to assist with assessment of key aspects of Health's management and operation of IT[1]. The audit builds on ANAO's earlier IT audits using CobiT[2].

10. Within the CobiT framework, IT governance is defined as a system of control that ensures that business objectives are achieved[3]. In order to provide the information that the organisation needs to achieve its objectives, IT governance must be exercised by the organisation to ensure that IT resources are managed by a set of naturally grouped IT processes[4]. Using selected CobiT processes, the ANAO examined IT governance at Health to determine whether Health's policies, practices, and procedures meet its business objectives. The CobiT processes reviewed by the ANAO were: *Managing IT Quality*, *Defining and Managing IT Service Levels*, *Ensuring IT Systems Security*, and *Monitoring the IT Processes*. Additionally, the CobiT component *IT Governance*, as the overarching structure that controls and links IT processes, resources and strategies, was included for review.

[1] The Information Systems Audit and Control Foundation and the sponsors of CobiT have designed the product primarily as an educational resource for computer control professionals. The Information Systems Audit and Control Association (ISACA) is the supporting worldwide organisation, comprised of control professionals and is based in the USA. CobiT is further discussed in Appendix 1. The Internet address for ISACA is <www.isaca.org>.

[2] The ANAO conducted the following audits of IT: ANAO Audit Report No.39 of 2000–2001, *Information Technology in Centrelink,* ANAO, Canberra, 2001. ANAO Audit Report No.44 of 2000–2001, *Information Technology in the Department of Veterans' Affairs,* ANAO, Canberra, 2001. ANAO Audit Report No.49 of 2000–2001, *Information Technology in the Health Insurance Commission,* ANAO, Canberra, 2001.

[3] Management Guidelines, CobiT, 3rd Ed., July 2000, p. 15.

[4] Management Guidelines, CobiT, 3rd Ed., July 2000, Appendix II: 'The CobiT Framework', p. 112.

11. The ANAO selected three major applications for evaluation, representing systems that process approximately $3.9 billion of expenditure, and tested those applications against the selected CobiT processes. A number of factors were considered in the selection criteria for applications, including financial expenditure, size of data holdings, critical effect on Health's business, and other current ANAO audits.

12. Two of the applications selected from Health were existing systems, that is, SPARC (System for Payments for Aged Residential Care) and ORAC (Office for Aboriginal and Torres Strait Islander Health Reporting Payments and Tracking System). The third application, SIME-1 (Strategic Information Management Environment), is a system under development intended to replace most of the existing systems at the Therapeutic Goods Administration (TGA). When completed, the system is expected to deliver the TGA with an information management framework, electronic commerce facilities and supportable electronic lodgement of data for entry of products onto the Australian Register of Therapeutic Goods. The selected applications are further described in Chapter 1.

13. In reviewing the applications, the ANAO evaluated the supporting procedures, standards and controls and performed appropriate tests, including transaction level testing (e.g. duplicate transactions, computational accuracy, tracing to source documents), in order to gain assurance that the applications could be relied upon to produce required outputs.

14. In pursuing the audit objectives, the ANAO applied selected CobiT components to consider whether Health's policies, practices and procedures were likely to meet its business objectives, through:

- meeting the IT customer requirements by planning, implementing and maintaining quality management standards and systems providing for distinct development phases, clear deliverables and explicit responsibilities (Managing IT Quality);
- establishing a common understanding of the required internal level of service through service level agreements, where these formalise the performance criteria against which the quantity and quality of service will be measured (Managing IT Service Levels);
- safeguarding information against unauthorised use, disclosure or modification, damage or loss by logical access controls, which ensure that access to the systems, data and programs is restricted to authorised users (IT Systems Security);
- monitoring the achievement of the performance objectives set for the IT processes by defining relevant performance indicators, the systematic and timely reporting of performance and by promptly acting upon performance problems (Monitoring IT Processes); and

- implementing a structure of relationships and processes to direct and control IT and its related processes (IT Governance).

15. The audit's conclusions are based on review against the CobiT criteria and an examination of the applications.

Overall audit conclusion

16. The ANAO concluded that, overall at the operational level, application systems reviewed during this audit are delivering the required business outputs in an effective and controlled manner, and within acceptable error rates. However, there are some unresolved department-wide IT governance issues that present risks to the optimal management and operation of IT.

17. The applications reviewed displayed a number of sound industry practices. The management and operation of IT taken as a whole also demonstrated compliance with better practice in a number of areas, but not consistently. At the time of the audit fieldwork, Health's IT governance arrangements did not have a department-wide process in place to ensure that better IT practice is consistently applied across the key IT areas of developing, implementing, and supporting systems, and monitoring IT performance. However, IT security was the exception as this was managed within a department-wide framework. Health's continuing development of a framework of better practice can assist the department to ensure consistency of approach to all IT activities. In addition, it can allow compliance with internal standards, quality requirements and service expectations as well as adherence to industry-accepted practices.

18. The ANAO further concluded that, overall, the application reviewed during this audit can be relied upon to achieve effective results. Extensive testing found the application data to be accurate, complete and consistent. The SPARC and ORAC systems are operating and being maintained in compliance with operational requirements established by Health. The SIME project is being developed in accordance with the project plan, with the exception of timing where there is a major delay. Recognising the project was not progressing according to the original target, the TGA put in place measures to address and manage the effect of the delays. The TGA also accepted a revised implementation date with the intention of ensuring full value from the project would be realised.

19. At the departmental level at the time of the audit fieldwork, Health did not have a requirement for internal IT quality or service delivery performance targets to be established, either for individual applications or IT as a whole. The absence of defined quality and service delivery targets at the departmental level potentially exposes Health to the risk that key IT customer or stakeholder requirements are not delivered, or continue to be delivered, to the required standard, in a timely manner.

20. For the applications reviewed, Health had implemented an appropriate level of management reporting to monitor the accuracy, completeness, consistency and currency of data. However, while monitoring of application data was taking place at the operational level, Health had not established overall performance objectives for IT at the department level. It had not defined key goal indicators, relevant performance indicators, and critical success factors for IT. Health had also not implemented internal or external benchmarking of IT. The absence of these performance indicators and targets, and benchmarking reduces Health's ability to monitor and measure the effectiveness, efficiency and economy of IT initiatives. It also limits the ability to produce systematic and timely reporting of IT performance.

21. The absence of a department-wide quality management framework, specification of service delivery targets, and monitoring of IT are the primary governance issues that must be addressed in order to ensure IT investments are optimised and that the gap between IT business risks, control needs and technical issues is bridged**.** The ANAO acknowledges that, as a result of Health's *IT Strategic Review*[5], the department had recognised these issues and was currently addressing them.

[5] During 2000–2001 Health commissioned consultants to examine the capability of the department to satisfy its current and future needs for information and services. The report from this review is referred to as the *IT Strategic Review.*

Key Findings

Managing IT Quality (Chapter 2)

22. In deriving a view on the principal issues of managing quality, the ANAO sought to identify:

- systems data, tested by the ANAO for accuracy, completeness, consistency, currency and uniqueness;
- overall responsibility for IT quality management within the department, in particular whether any group within Health had a defined role in setting quality management practices and processes;
- documentation of IT quality management policies within Health; and
- information on the practices and processes of the teams developing or making changes to IT systems.

23. The ANAO found that overall the SPARC and ORAC applications data tested during this audit exhibit quality characteristics. The data tested was found to be accurate, complete and consistent, and reflected source documents. All payments tested had appropriate segregation between certification and authorisation for payment, and authorisations were within the approved delegations. Minor improvement opportunities were noted in order to maintain and/or strengthen application data quality.

24. However, the SIME-1 development was running approximately 18 months behind schedule for one of the major phases. Delays have resulted in the lost opportunity for TGA staff to work on other projects and in the TGA realising the benefits of the new system according to the original schedule. Recognising the project was not progressing according to the original target, the TGA put in place processes to address and manage the effect of the delays. The TGA also accepted a revised implementation date with the intention of ensuring full value from the project would be realised.

25. The ANAO further found that, at the time of the audit, Health had not established at the departmental level an overarching quality culture or implemented a systematic framework of quality control responsibilities and practices, including quality assurance reviews. Health was not consistently applying system development methodologies and programming standards, as it did not have a current methodology. The absence of a department-wide quality framework limits Health's ability to ensure IT investment decisions adhere to the requirements of quality standards, and that information produced through IT initiatives continue to meet the business needs.

26. The ANAO found that Health did not have a quality assurance knowledge base. A knowledge base contains longitudinal and comparative data on the performance of IT. It can be used as a reference tool of qualitative and quantitative data to assist with continuous improvement of IT within the department. Setting measures for the success of developments, and using those measures as the basis for evaluating both the success and the quality of the development may facilitate development of such a knowledge base. Over time, a reference tool can be created for Health's internal benchmarking that will allow assessment of whether quality goals have been and are being achieved.

27. During fieldwork the ANAO found that Health conducts no internal benchmarking of its management of IT or implementation of IT initiatives. Health did not benchmark against the IT industry generally, or against similar Commonwealth agencies. Internal benchmarking allows an organisation to identify better practices internally; external benchmarking allows the organisation to compare its efficiency and effectiveness against other organisations.

28. The ANAO noted that Health's *IT Strategic Review* identified the need to establish a quality framework. The ANAO acknowledges that Health was in the process of developing department-wide processes by which the overall quality of business information produced through IT initiatives can be assessed. Subsequent to the findings of the *IT Strategic Review*, Health was developing a framework of quality policies and standards to guide IT development efforts.

Managing IT Service Levels (Chapter 3)

29. In coming to a view on the principal issues of defining and managing service levels, the ANAO sought to determine if service delivery parameters had been established between the BSB and owners of the three business applications included in this audit.

30. The SPARC and ORAC systems are operating and being maintained within operational requirements, even though there is an absence of department-wide defined internal service delivery performance measures. As a system under development, the SIME project was not tested. Processing with these applications was timely and accurate, and in accordance with the general business rules outlined in key legislation and Health policies.

31. At the departmental level, Health did not routinely use internal service delivery targets or service level agreements to define and prescribe the quantity and quality of service delivery. The ANAO found that, while there were no documented definitions of responsibilities between the Business Systems Branch and system owners, there are practices and agreements, on a project by project basis, that recognise the different responsibilities for managing IT service levels, project deliverables, time frames, and cost estimates. Following from a recommendation of the Corporate Activities Review, Health was in the process of developing internal service level arrangements, and the management and reporting of internal service level expectations.

32. Any assurance on the integrity of a project deliverable will depend on the quality of the deliverable. Quality is assured by a consistent, planned and enforceable quality assurance process. Such a process did not exist at the departmental level within Health at the time of the audit. The ANAO found that Health did not have a prescribed process in place to establish and assess the criteria upon which customer satisfaction could be measured.

IT Systems Security (Chapter 4)

33. In coming to a view on the principal issues of ensuring systems security, the ANAO sought to determine the existence or otherwise of:

- Health's policies and procedures for system security and access;
- documents and/or reports of IT security activities including, but not limited to, internal audit reports, user reports and any other assessments of Health's security management of IT resources;
- the currency of application security plans;
- tools or procedures used for monitoring security compliance, breaches and reporting;
- centralised security responsibilities; and
- user account management and logical access control mechanisms.

34. Health effectively manages its IT security, with appropriate security controls and compliance/monitoring procedures having been implemented. The maintenance of an appropriate security environment is an essential departmental activity, given the importance of preserving the confidentiality and privacy of data holdings within Health. For the SPARC and ORAC applications, the ANAO assessed segregation of duties, access controls, and authorisations, and found these to be effective.

35. Subsequent to completion of the audit fieldwork, the ANAO has conducted additional IT security and disaster recovery testing as part of the financial statement audit process. No issues were identified. At the departmental level, good levels of security awareness exist, and responsibilities for IT security are clearly assigned, managed and enforced.

36. The ANAO found that an IT&T Security Policy had been established by Health in order to implement and manage its security requirements. The Contestability Branch monitors audit logs for potential breaches of security. Where breaches appear to have occurred, an explanation is requested of the relevant officer. Where usage is inappropriate, the Branch head is advised. Health prosecutes serious breaches, specifically incidents of fraud.

37. Health's policy requires a system security plan to be developed and maintained for each application system. This is an example of good practice. There is a further requirement for the plan to be amended if changes are made to the underlying application system. The ANAO found that the SPARC and ORAC Security Plans were not signed off, but during the course of the audit Health took action to finalise the plans. The security plan for SIME was found to be very comprehensive and detailed in its coverage.

38. Because of the nature of the data collected, held and processed within Health's IT systems, the confidentiality and privacy of information are important business issues. Although designated responsibility for privacy matters, at the commencement of this audit the Information Planning and Privacy Committee (IPPC) had not developed policy or guidelines to ensure compliance with the information privacy principles of the Privacy Act. Since that time, the IPPC has allocated a task to a subcommittee to address privacy issues with a completion date of June 2002.

39. The ANAO's review of application security plans indicates that information privacy requirements have not been adequately addressed as none of the plans reviewed had considered privacy issues.

40. Improvement opportunities were identified in the content and timeliness of completion of individual system security plans, and in the practice of using production data (that contains personal information) for testing purposes. Some plans may need revising to address privacy concerns identified by the IPPC work program.

Monitoring IT Processes (Chapter 5)

41. In considering the principal issues of monitoring the processes, the ANAO sought to determine the existence or otherwise of:

- policies and procedures relating to monitoring and reporting on IT performance;
- documents and/or reports of IT activities including, but not limited to, internal audit reports, user reports, user satisfaction surveys, committee minutes and any other assessments of Health's use of IT resources;

- key performance indicators and / or critical success factors used to measure IT performance;
- data used for monitoring IT resources and the appropriateness of the data collected; and
- the existence and timeliness of IT performance management review processes.

42. At the operational level, Health effectively monitored the data of the SPARC and ORAC systems for accuracy, completeness, consistency, currency and uniqueness, and appropriate arrangements were in place to produce and review reports to management. As the SIME project was under development, monitoring procedures had not been developed, but this was an identified project task.

43. While operational monitoring of data was taking place, at the department-wide level Health did not routinely use key goal indicators, key performance indicators and critical success factors to measure and report on the efficiency and economy of IT processing. It did not have performance targets (scorecards) for IT, nor did it undertake customer satisfaction assessments.

44. As previously mentioned in the key findings for the chapter on Managing IT Quality, the ANAO found that Health did not engage in any benchmarking of its IT function against external organisations in order to assess the overall effectiveness of IT activities. Benchmarking is relevant to both quality and monitoring. However, Health did use a standard industry measurement, function point analysis, to measure the size of its applications.

45. Consistent with the recommendations of the *IT Strategic Review,* Health is developing policies and procedures for monitoring and reporting on IT performance. It is establishing performance targets for IT and implementing internal and external benchmarking.

46. The ANAO found that, at the operational level, financial and timeliness targets were set for significant changes to systems and for new system developments. Although important, these targets alone do not indicate the overall success of a change or development project. Customer satisfaction, both within Health (the system users) and external to Health (e.g. residential care facilities and recipients of grants) is a major indicator of the success of IT systems. The ANAO found surveys of internal or external users of the systems were not conducted as part of a regular process. The ANAO was subsequently informed that a user survey was part of a formal post implementation review for ORAC in 1998.

47. Internal Audit had conducted a number of audits of aspects of IT in recent years. Internal Audit's activities are generally addressed through Internal Audit representation on steering committees. Health's Audit Committee appropriately considered the reports of the audits and ensured recommendations were addressed.

IT Governance (Chapter 6)

48. In coming to a view on the principal issues of IT governance, the ANAO focussed on those aspects of IT governance at Health that were most likely to have a significant impact upon the overall achievement of business objectives, specifically:

- the role of the DMC in relation to IT governance issues;
- the roles of and relationship between the Information Planning and Privacy Committee (IPPC) and the Information Technology Committee (ITC);
- responsibility for progressing the recommendations of the *IT Strategic Review*; and
- the internal audit work program.

49. The ANAO found that Health had established IT governance committee structures during 2000 as an integral part of overall governance arrangements within the department. Notwithstanding, at the commencement of the audit, Health had yet to fully implement department-wide IT management practices that ensured consistency with accepted best practice and optimal use in the management and operation of IT.

50. Recognising the need to further revise IT governance, Health commissioned the *IT Strategic Review* in late 2000 to ensure that the department had the capability to satisfy current and future needs for information and services. The report from this review, released in mid-2001, identified a number areas of concern in terms of IT structures and processes, and made a number of recommendations to address these concerns. Health is in the process of addressing the recommendations.

Health’s response

51. Health agreed with the recommendations made in the report and commented:

> The Department had also recognised the lack of an appropriate quality framework and system development methodology to guide its system development efforts. In 2001, it initiated the IT Strategic Review to identify an appropriate mechanism for their delivery, together with a more effective organisational structure and process model.

The Department agrees with the ANAO that, at the time of the audit, the structure, process and model were not in place, and is pleased to see that the report recognises the work that has been completed in this area and the extent to which implementation of the recommendations of the IT Strategic Review will ensure a robust governance and IT development framework for delivery of business systems to the Department.

It is recognised, of course, that both the Project Lifecycle and Quality Framework will continue to evolve and that the continuous improvement process will enable the Department to further develop the processes to meet the critical success factors and goal indicators of the CobIT.

Recommendations

Set out below are the ANAO's recommendations, with report paragraph references and an indication of Health's response. The recommendations and responses are discussed at the relevant parts of this report.

Recommendation No. 1 Para. 4.35

The ANAO recommends that Health:

- review the content of all application security plans, using the SIME security plan as an example of sound practice, to ensure Health's security requirements have been fully addressed;
- include privacy requirements in security plans; and
- ensure that for any production data used in test environments, the data does not include identifiable personal information.

Health's response: Agreed.

Recommendation No. 2 Para. 5.39

The recommendations of Health's *IT Strategic Review* provide a blueprint for improving overall IT management within the department. The ANAO recommends that Health set and meet a firm timetable for implementation of the Review's recommendations relating to:

- completion of the IT Quality Framework and system development methodologies;
- the development of service delivery targets and service level arrangements between BSB and client divisions; and
- developing a program for measuring and benchmarking the performance of its IT, including measures to assess the success or otherwise of IT projects.

Health's response: Agreed.

Audit Findings and Conclusions

1. Introduction

This Chapter provides an overview of the Department of Health and Ageing, and it discusses the scope and rationale for those aspects of Health's information technology reviewed in this audit. The Chapter also describes the audit objectives, methodology and the structure of the report.

The Commonwealth Department of Health and Ageing

1.1 The Department of Health and Ageing *(hereinafter referred to as 'Health')* has a diverse range of responsibilities, which include promoting good health, ensuring all Australians have access to key health resources and promoting quality aged care services. Health's vision is 'a world class health and aged care system for all Australians'. Health aims to achieve this vision through its nine portfolio outcomes that include:

- population health and safety;
- quality health care;
- enhanced quality of life for older Australians; and
- Aboriginal and Torres Strait Islander health.

1.2 The total appropriation for Health in 2001–2002 was approximately $29 billion. For 2001–2002, the Parliament appropriated $794 million for Health's departmental outputs and $28.3 billion for its administered outputs.

1.3 A range of government programs are administered by the HIC on behalf of Health, including Medicare, the Pharmaceutical Benefits Scheme (PBS), aspects of the 30 per cent Private Health Insurance rebate and payments to hearing service providers. In 2001–2002, payments to the HIC are estimated to be $14.7 billion and represent nearly 52 per cent of Health's administered funding.

1.4 Health also provides a substantial amount of funding in the form of Specific Purpose Payments to the States and Territories. The largest of these is the Australian Health Care Agreements (estimated at $6.7 billion for 2001–2002).

1.5 Health employs around 3500–3600 staff, the majority of whom are located in Canberra and other staff who are principally situated in capital cities.

Information Technology at Health

1.6 Health's IT environment is complex and the department relies considerably on IT to achieve its business objectives.

1.7 Health has outsourced administrative and operational responsibility for its IT infrastructure services, including mainframe and server administration and management. In June 2000, IBM-GSA was contracted to provide Health's IT infrastructure, in accordance with the Government's objectives of market testing all departmental IT infrastructure services. The IT outsourcing at Health was included in a group that also included the HIC and Medibank Private.

1.8 The outsourcing contract provides for the outsourcer to manage the configuration and operation of the computer mainframes and servers, including as required, change management, security configuration, privileged user access and the business resumption plan. While Health purchases IT infrastructure services, it retains responsibility for ensuring that effective controls are in operation.

1.9 Health invests a significant amount of funds into IT, for example:

- the written down value of software developed and in operation at 30 June 2001 was $43 million, including $3.5 million of externally purchased software; and
- expenditure in 2000–01 for IT infrastructure services of $48 million, including a one-off transition cost payment of $19 million to the department's principal service provider.

1.10 Health holds large amounts of data, including all records of medical benefit claim payments since July 1975. Health is responsible for the security and privacy of these data. Health currently maintains an extensive range of applications in order to support the diverse activities and programs managed within the department. These applications reflect both internally developed and purchased mainframe and client-server network applications.

1.11 Health is a major user of document and file management systems, e-mail (internal and external), electronic business systems, and the Internet. Health has a number of IT systems, linked electronically to the financial and human resource management system (SAP). Health also has a number of systems for managing the payment of grants.

1.12 There is a nightly exchange of data with other organisations that assist with Health's IT functions. This exchange of data is integral to payment processes and advice to stakeholders.

1.13 On the basis of its status as a major department with a large IT investment, Health was selected by the ANAO for an audit of its management and operation of IT.

Audit objectives

1.14 The overall objectives of the audit were to determine whether Health's management and operation of selected IT systems:

- meet industry better practice;
- meet quality and service delivery parameters set by Health and, if applicable, by the Government; and
- operate effectively, efficiently and economically.

Audit methodology and scope

1.15 The overall quality of service delivery and achievement of departmental outcomes is affected significantly by the accuracy of application processing. Health has numerous IT systems, some large, some small. The ANAO selected three major applications for evaluation, representing systems that process approximately $3.9 billion of expenditure, and tested those applications against selected components of an IT standards framework. A number of factors were considered in the selection criteria for applications, including financial expenditure, size of data holdings, critical effect on Health's business, and other current ANAO audits.

1.16 The first of these current ANAO audits is examining the administrative effectiveness of arrangements between Health and the HIC in relation to delivering Medicare and the Pharmaceutical Benefits Scheme, and the implementation of Health's and the HIC's strategic partnership agreement. The second audit is reviewing performance information under Australian Health Care Agreements. These agreements provide federal funding for public hospitals in the states and territories at a cost of $6.7 billion in 2001–02.

1.17 The three major applications selected for evaluation were as follows:

- ***SPARC***: System for Payments for Aged Residential Care. SPARC is the supporting application responsible for the payment of funds to residential aged care facilities. Health's expenditure through SPARC in 2001–02 is estimated to be $3.7 billion.
- ***ORAC***: OATSIH (Office for Aboriginal and Torres Strait Islander Health) Reporting Payments and Tracking System. ORAC is the supporting application for grant and payment management for Aboriginal and Torres Strait Islander health services. Health's expenditure through ORAC in 2001–02 is estimated to be $178 million. Most ORAC payments are to indigenous community-controlled health organisations throughout the country.
- ***SIME-1***: Strategic Information Management Environment. SIME is a major application currently under development for the Therapeutic Goods Administration (TGA). With the operation of SIME, the TGA intends to implement an information management framework, provide electronic commerce facilities and supportable electronic lodgement of data for entry

of products onto the Australian Register of Therapeutic Goods. The development and implementation of SIME is being achieved through a series of projects, each consisting of several separately defined subprojects or phases. SIME-1 is the current project and it consists of 11 phases. Eventually the majority of existing applications at the TGA will be replaced by SIME. Annual turnover through SIME will be approximately $51 million.

1.18 In reviewing the applications, the ANAO evaluated the supporting procedures, standards and controls and performed appropriate tests, including transaction level testing (e.g. duplicate transactions, computational accuracy, tracing to source documents), in order to gain assurance that the applications could be relied upon to produce required outputs. By testing the data and outputs of selected applications, the audit determined whether:

- the applications could be relied upon to produce required outputs accurately and whether error rates were within acceptable, pre-determined levels;
- agreed internal service levels between the service provider and the system owners were in place and performance measures were being met;
- appropriate security and access restrictions were in place; and
- departmental monitoring of performance objectives for IT processing was timely and accurate.

1.19 The audit applied selected components of CobiT (Control Objectives for Information and Related Technology), a framework of internationally accepted standards to assist with assessment of key aspects of Health's management and operation of IT[6]. The Information Systems Audit and Control Foundation developed CobiT as a generally applicable and accepted standard for good practices for IT control. It provides a framework of 34 high-level control processes for each defined IT process and, by addressing the control processes, enables a business owner to assess that its IT is adequately controlled. Table 1 lists the entire scope of the CobiT IT process framework and the processes selected for examination in this audit. The audit builds on ANAO's earlier IT audits using CobiT. For example, during 2001 the ANAO conducted audits of IT at Centrelink[7], the Department of Veterans' Affairs[8] and the Health Insurance Commission[9] and respective audit reports were issued.

[6] The Information Systems Audit and Control Foundation and the sponsors of CobiT have designed the product primarily as an educational resource for computer control professionals. The Information Systems Audit and Control Association (ISACA) is the supporting worldwide organisation, comprised of control professionals and is based in the USA. CobiT is further discussed in Appendix 1. The Internet address for ISACA is <www.isaca.org>.

[7] ANAO Audit Report No.39 of 2000–01, *Information Technology in Centrelink,* ANAO, Canberra, 2001.

[8] ANAO Audit Report No.44 of 2000–01, *Information Technology in the Department of Veterans' Affairs,* Canberra, 2001.

[9] ANAO Audit Report No.49 of 2000–01, *Information Technology in the Health Insurance Commission,* Canberra, 2001.

1.20 The ANAO selected the CobiT components of *Managing IT Quality, Defining and Managing IT Service Levels, Ensuring IT System Security* and *Monitoring the IT Processes* for review during this audit. Additionally, the CobiT component *IT Governance* was included for review as the overarching structure that controls and links IT processes, resources and information to Health's departmental strategies and objectives.

1.21 The ANAO applied selected CobiT components to consider whether Health's policies, practices and procedures were likely to meet its business objectives, through:

- meeting the IT customer requirements by planning, implementing and maintaining quality management standards and systems providing for distinct development phases, clear deliverables and explicit responsibilities;[10]
- establishing a common understanding of the required internal level of service through service level agreements, where these formalise the performance criteria against which the quantity and quality of service will be measured;[11]
- safeguarding information against unauthorised use, disclosure or modification, damage or loss by logical access controls, which ensure that access to the systems, data and programs is restricted to authorised users;[12]
- monitoring the achievement of the performance objectives set for the IT processes by defining relevant performance indicators, the systematic and timely reporting of performance and by promptly acting upon performance problems;[13] and
- implementing a structure of relationships and processes to direct and control IT and its related processes.[14]

[10] Management Guidelines, CobiT, 3rd Ed., July 2000, IT Process PO11: *'Manage Quality' (Planning and Organisation),* p. 44.

[11] Management Guidelines, CobiT, 3rd Ed., July 2000, IT Process DS1: *'Define and Manage Service Levels' (Delivery and Support),* p. 62.

[12] Management Guidelines, CobiT, 3rd Ed., July 2000, IT Process DS5: *'Ensure Systems Security' (Delivery and Support),* p. 70.

[13] Management Guidelines, CobiT, 3rd Ed., July 2000, IT Process M1: *'Monitor the Processes' (Monitoring),* p. 90.

[14] Executive Summary, CobiT 3rd Ed., July 2000, Executive Overview, p. 3.

Table 1

Control Objectives for Information and Related Technology: Process and Control Objectives[15]

		Information Criteria[16]							
	CobiT Process and Control Objectives	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	Addressed in this audit
	Planning and organisation								
P01	Define a strategic IT plan	P	S						
P02	Define the information architecture	P	S	S	S				
P03	Determine the technological direction	P	S						
P04	Define the IT organisation and relationships	P	S						
P05	Manage the IT investment	P	P					S	
P06	Communicate management aims and direction	P					S		
P07	Manage human resources	P	P						
P08	Ensure compliance with external requirements	P					P	S	
P09	Assess risks	P	S	P	P	P	S	S	
P10	Manage projects	P	P						
P11	Manage quality	P	P		P			S	✓
	Acquisition and implementation								
AI1	Identify solutions	P	S						
AI2	Acquire and maintain application software	P	P		S		S	S	
AI3	Acquire and maintain technology architecture	P	P		S				
AI4	Develop and maintain IT procedures	P	P		S		S	S	
AI5	Install and accredit systems	P			S	S			
AI6	Manage changes	P	P		P	P		S	
	Delivery and support								
DS1	Define service levels	P	P	S	S	S	S	S	✓
DS2	Manage third party service	P	P	S	S	S	S	S	
DS3	Manage performance and capacity	P	P			S			
DS4	Ensure continuous service	P	S			P			
DS5	Ensure systems security			P	P	S	S	S	✓
DS6	Identify and attribute costs		P					P	
DS7	Educate and train users	P	S						
DS8	Assist and advise IT customers	P	P						
DS9	Manage the configuration	P				S		S	
DS10	Manage problems and incidents	P	P			S			
DS11	Manage data				P			P	
DS12	Manage facilities				P	P			
DS13	Manage operations	P	P		S	S			
	Monitoring								
M1	Monitor the process	P	P	S	S	S	S	S	✓
M2	Assess internal control adequacy	P	P	S	S	S	P	S	
M3	Obtain independent assurance	P	P	S	S	S	P	S	
M4	Provide for independent audit	P	P	S	S	S	P	S	

[15] Audit Guidelines, CobiT, 3rd Ed., July 2000, p. 29.

[16] P = a primary criteria addressed by the process, S = a secondary. A blank cell indicates the process does not address the information criteria.

1.22 Examination of all aspects of Health’s IT against all CobiT components was considered as an option and not pursued because it would have extended the audit beyond acceptable time and cost parameters for performance audits. The proposal was to use selected CobiT components that would allow the audit team to draw specific conclusions against those components, while drawing general conclusions against the management and operation of Health’s IT as a whole. The specific CobiT components selected for review were those considered critical to the satisfactory management and operation of IT within Health. The ANAO extended the standard CobiT approach to review IT governance.

1.23 The ANAO conducted fieldwork between September 2001 and January 2002, predominantly at Health’s National Office in Canberra and also at Health’s state offices in New South Wales, Victoria, Queensland, and South Australia.

1.24 The audit drew on and extended the work undertaken by the ANAO as part of Health’s 2000–01 and 2001–02 financial statement audit process. Fieldwork in state offices was performed in conjunction with the financial statement audit.

1.25 The audit was conducted in accordance with ANAO Auditing Standards. Its cost was $320 000.

Report structure

1.26 The remainder of this report presents the ANAO’s audit findings, conclusions and recommendations on specific aspects of IT at Health. The presentation of the report broadly follows the CobiT framework adapted to this audit:

- Managing IT Quality (Chapter 2);
- Managing IT Service Levels (Chapter 3);
- IT Systems Security (Chapter 4);
- Monitoring IT Processes (Chapter 5); and
- IT Governance (Chapter 6).

2. Managing IT Quality

This Chapter examines Health's policies, practices and procedures used to meet the IT quality management requirements of the department. It reports audit findings on current quality standards and the results of tests of quality measures.

Quality

2.1 For all public and private sector organisations using IT, increasing reliance upon IT for the achievement of business objectives has generated a need to manage the quality of IT to ensure value for money. An IT quality assurance (QA) framework and management process ensures that:

- business information produced through IT initiatives is accurate and timely; and
- development, implementation, operation, and maintenance of IT applications meet the business needs through complying with a set of quality standards.

2.2 Appendix 2 includes the CobiT definition, along with specific control objectives, critical success factors, key performance indicators and key goal indicators, for *Manage Quality*.

Audit approach

2.3 The ANAO tested the selected applications for data quality management, including data entry and transaction processing preparation, validation and editing; duplicate transactions; system calculations; control totalling, output balancing and reconciliation procedures; and source document control and retention.

2.4 In addition, the following CobiT principles for manage quality were considered[17]:

- *establishment of a quality culture;*
- *quality assurance responsibilities;*
- *quality control practices;*
- *system development life cycle methodology;*
- *quality assurance reviews and reporting;*

[17] Audit Guidelines, CobiT, 3rd Ed., July 2000, IT Process PO11: *'Manage Quality' (Planning and Organisation)* p. 84.

- *development of a quality assurance knowledge base; and*
- *benchmarking against industry norms.*

2.5 In coming to a view on the principal issues of managing quality, the ANAO sought to identify:

- systems data, tested by the ANAO for accuracy, completeness, consistency and currency;
- overall responsibility for IT quality management within the department, in particular whether any group within Health had a defined role in setting quality management practices and processes;
- documentation of IT quality management policies within Health; and
- information on the practices and processes of the teams developing or making changes to IT systems.

Quality management at Health

2.6 Individual application system quality is the overall responsibility of each system owner. System owners are the heads of the divisions that are responsible for the relevant systems, and their responsibilities are defined in the Chief Executive Instructions (CEIs).

2.7 The BSB had department-wide responsibility for IT quality assurance within Health. The BSB did not have the authority to examine the quality of systems in development unless invited to do so by the system owners. The BSB did not review systems for meeting programming or system documentation standards.

2.8 The BSB, however, chairs the Technical Environment Change Control Committee (TECC). Health and IBM-GSA jointly staff this Committee. The Committee has a major role in providing a final review of changes prior to approval and implementation, as well as ensuring documentation standards are met before changes to production systems are allowed.

Audit findings

Applications testing

SPARC application: Data entry

2.9 The ANAO tested the quality of data entry procedures for the SPARC application and detected a number of minor data entry errors. However, the overall number of errors was statistically small and none of the detected errors resulted in materially incorrect payments. Data entry procedures are considered adequate and current control practices that include, for example, a 10 per cent random check on all claims as well as a claim certification process, minimises the risk of incorrect payments being made through data entry errors.

SPARC application: Timing of post-implementation reviews

2.10 The ANAO found that the SPARC project team conducted post-implementation reviews (PIRs) after each application change release. This is a positive control procedure to ensure implementation objectives have been satisfied. PIRs focus on the identification of successful and unsuccessful results so that lessons learnt can be applied to future releases. However, the ANAO found that PIRs are generally conducted within five days of release, but a month or more might pass before errors appear in the operation of the system. Since raising this issue and completion of the audit fieldwork, a two-stage review process has been established, the first stage within five days and the second stage four weeks after implementation to ascertain how the new functionality impacts the business process.

ORAC application: Payments process

2.11 The funding agreements between Health and indigenous health services providers require the recipient of Commonwealth funds to satisfy various performance criteria, one of which is the furnishing of financial statements at regular intervals. Ongoing payments are contingent upon the recipient satisfying the performance requirements.

2.12 The ANAO found that the ORAC system was not used to automatically prevent payments when the indigenous health service providers did not meet performance requirements. Difficulties in implementing an automated control led to a business decision being made to exclude this feature from the system, and manual processes being implemented within each State/Territory office. The ANAO considers that the manual process would be strengthened by inclusion of a system-enforced preventative control. Health advised the ANAO that this feature would be included in the system to replace ORAC, expecting to be implemented in 2003.

ORAC application: Date controls

2.13 In a payment process, date controls reduce the risk of inappropriate payments being made. Without adequate controls over separation of procedures by date, there is a risk that payments might be made before authorisation of the payments. The ANAO examined the ORAC business process for the management of payments to indigenous health service providers. The dates entered into ORAC reflect key milestones in the business process that generally reflect sequential events. The ANAO examination of ORAC dates observed that some funding acceptance dates were after funds payable dates, the same date was recorded for all milestones for some providers, and no milestone dates were listed for some providers in an ORAC management report.

2.14 The ANAO discussed the observations with Health. Health’s investigations identified the need to clarify the interpretation of some key dates, and it provided such clarification to staff. Health advised that payments can not be made prior to date of acceptance of the funding agreement and payments are only created after the date of acceptance is recorded in the system. ANAO testing confirmed appropriate controls were in place and no incorrect payments had been made.

SIME application: Timeliness of project delivery

2.15 The ANAO found that the SIME-1 development was running approximately 18 months behind schedule for one of the major phases. While work on subsequent phases was able to continue, there was a dependency on implementation of the delayed phase. Implementation of each phase is progressing, and full implementation of all phases is now expected by December 2002, against the original target of August 2001. The ANAO noted that, before being awarded the contract, the successful tenderer was provided with funding for a proof of concept and business familiarisation. Funding was to provide additional assurance that the proposed solution was viable and that all business requirements would be satisfied. No changes were made to the proposed solution as a result of this exercise. The ANAO considers that there is no single cause of the delay. The project was not subject to any significant change of scope. Contributing to the delays were:

- changes in the contractor’s project manager;
- TGA’s insistence that project deliverables met their quality objectives and all business requirements. The contractor advised that it always agreed with and sought to meet those expectations;
- TGA’s agreement to changes in the technical options for delivery of the system to provide a better solution; and
- the contractor’s underestimation of the complexity of TGA’s business processes, and therefore the solution to meet business requirements.

2.16 Recognising the project was not progressing according to the original target, the TGA put in place processes to address and manage the effect of the delays. The TGA also accepted a revised implementation date with the intention of ensuring full value from the project would be realised.

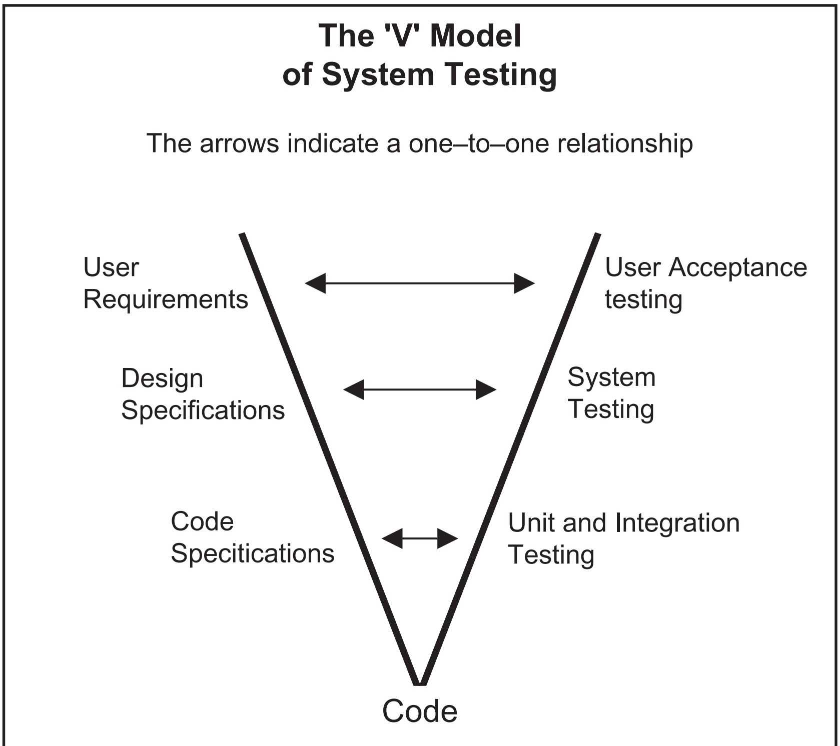
2.17 The project was based on a fixed price contract. Progress payments to the contractor were made depending on the completion of individual phases, with 25 per cent of the contracted price of each phase held until completion of the total project. Delays have resulted in the lost opportunity for TGA staff to work on other projects and in the TGA realising the benefits of the new system according to the original schedule. A resulting benefit of the delay has been that recent legislative changes have been incorporated into project deliverables, and thus reduce the need for a major enhancement shortly after implementation.

SIME application: Matching business requirements with testing

2.18 The ANAO tested the linkage between the SIME business requirements, and user acceptance testing (see Figure 2.1). The ANAO found an appropriate linkage between business objectives, system and unit specifications and system and user testing. The ANAO concluded that a satisfactory audit trail for tests had been maintained.

Figure 2.1

Requirements and testing linkage



Source: Health and ANAO discussions

Quality culture

2.19 The ANAO did not find evidence that Health had established an overarching quality framework and/or quality standard either for the department as a whole, or for IT within the agency. A quality framework helps ensure IT investment decisions adhere to set standards and methodologies, and promote a continuous improvement philosophy to achieve business objectives.

2.20 With the exception of the SIME development, the ANAO found that application developments and major changes to applications did not include a plan to address IT quality issues as part of the process. Quality plans define the testing and assurance processes that ensure the IT system meets the stated business requirement, that deliverables are of a high standard, and that agreed quality procedures and guidelines are adhered to. Health's IT Strategic Plan for 2000–2002 identified quality standards for system developments to be developed by October 2000. These standards were still being developed at the time of this audit.

2.21 Following the fieldwork for the audit, Health advised that an IT Quality Framework was being developed with an expected implementation date of April 2002. The *IT Strategic Review* had identified the need to establish a quality framework. Appendix 2 describes the CobiT defined critical success factors that would indicate existence of an overarching quality framework.

Quality assurance responsibilities

2.22 At the time of the audit, while Health had assigned responsibility at the operational level for individual application systems, Health had not identified overall departmental responsibility for quality management, other than that the BSB was responsible for performing a quality assurance function.

2.23 The BSB conducts quality assurance tasks, if requested by divisions, and at a cost to the requesting division. The ANAO found that from a quality assurance perspective the BSB had minimal participation in system development or maintenance projects. Minimal participation in quality assurance activities increases the risk that poor quality practices are not identified and improved, and good quality practices are not disseminated throughout Health. In terms of quality assurance the BSB:

- had no involvement in quality assurance of two significant applications (SPARC and ORAC) and has not been involved in the SIME development;
- did not necessarily participate in critical phases of system development efforts that contribute to quality, (e.g. user testing and PIRs);

- did not participate in maintaining quality standards associated with the system development life cycle methodology (SDLCM); and
- did not monitor the project teams' adherence to standards of programming.

2.24 Since completion of the fieldwork, Health advised the ANAO that, as part of the reorganisation of the Business Systems Branch resulting from the recommendation of the *IT Strategic Review*, a separate section has been created (Quality Management Section) with responsibility for quality management of IT in Health. The section has been responsible for the development of the Quality Framework document and also has responsibility for:

- configuration management;
- BSB standards and procedures; and
- provision of test management services.

2.25 Quality assurance activities can assist Health to meet its obligations under the FMA Act. The ANAO considers that in discharging its role to ensure quality, it would be appropriate for the BSB to seek the advice of Internal Audit (as Health's independent advisor on IT risks and controls) in developing its quality assurance process and procedures. Additionally, there could be a role for Internal Audit in ensuring compliance with the quality assurance program implemented by BSB.

Quality control practices

2.26 The ANAO found that system development and change management processes for the systems reviewed included elements that contributed to the overall quality of the information delivered. The best example of this was in the SIME development by the TGA, the project planning of which included a plan to address IT quality issues for the project, as well as independent quality assurance. Other examples are post-implementation reviews and testing of systems being developed or changed.

2.27 The ANAO also found that Health did not adhere to a consistent quality management framework or methodology in developing or maintaining systems. Project teams embraced a number of control practices, however, that contribute to quality management within each application development or change process. Current control practices include conducting systematic system testing of programs, structured change management processes, and post-implementation reviews.

2.28 The ANAO noted that the *IT Strategic Review* identified areas for change with business systems analysis at Health. Business analysis is the process whereby the development team produces a specification that states the functional and data requirements for a new system. The ANAO found the SIME project business systems analysis to be satisfactory.

2.29 The ANAO found that Health did not have a single preferred tracking system to identify the status of all applications under development. For example, the TGA's development of SIME is external to the jurisdiction of the BSB, and its development would not be reflected in Health's general tracking system for IT developments. Applications developed without ITC approval would also not be represented. (This current audit did not identify any developments in this situation.) Without a departmental-wide perspective on systems under development, there is a risk that management decision-making, resource allocation, and cost considerations may be inefficient or ineffective. The ANAO noted that the *IT Strategic Review* identified a number of similar concerns.

2.30 Since completion of the audit, Health advised the ANAO that, as part of the reorganisation of Business Systems Branch resulting from the recommendations of the *IT Strategic Review*, a new separate section, mentioned earlier in this chapter, will also have responsibility for development of a tracking system to identify and monitor the status of all systems under development. That tracking system has now been implemented.

System development life cycle methodology (SDLCM)

2.31 At the time of the audit, Health had not established a uniform, mandatory system development and project management methodology. Two SDLCMs were available simply as reference guides for development. For consistency, Health's system development processes must align with IBM-GSA's procedures.

2.32 A standard system development methodology governing the process of developing, acquiring, implementing, and maintaining information systems will assist Health to better manage the risks of:

- projects not matching business needs;
- necessary procedures not being undertaken or controls not implemented;
- applications being developed or changed unsystematically, inefficiently or ineffectively;
- inefficient use of resources; and
- consequential, unnecessary costs being imposed.

2.33 Of the two current SDLCMs, the Systems Administration Method was developed in 1991. The methodology is outdated and not widely used, mainly because it is a series of rigid, predefined development stages rather than an iterative process. The Aged and Community Care Division is the principal group using the other methodology, titled Rapid Application Development.

2.34 Since completion of the fieldwork for this audit, Health advised the ANAO that the *IT Strategic Review* recommended a process approach to applications development and maintenance with an organisational structure and process mirroring the traditional stages of an SDLCM. The organisational structure and processes have recently been implemented. The BSB has now developed a system development methodology document, the Project Lifecycle. This describes the phases, processes and deliverables involved in the development, implementation and support of applications within Health. Adherence to the methodology will be verified as a precondition for implementation of a system release, once Health approves the methodology.

2.35 Health advised that the systems development methodology document, Project Lifecycle, is now available on the Intranet to all departmental staff. No formal training in the use of the methodology is planned, however instruction, assistance and advice to individuals and workgroups are available when IT projects are undertaken. Internal Audit has been consulted in regard to the inclusion of risk management and internal control considerations.

2.36 The ANAO found that the SPARC and ORAC applications did not have centrally accessible and up-to-date system documentation. However, documentation for current change processes for the SPARC and ORAC applications was satisfactory. In particular, the SPARC documentation was found to be of a high standard. Adherence to a standard development methodology would increase the probability that systems documentation was developed and maintained, while insufficient documentation increases the risk of errors being introduced in maintenance activity or result in the inability to support the system.

2.37 The SIME project is producing and maintaining a high level of systems documentation. The project continues to produce a clearly referenced audit trail for all project activities, from inception through user acceptance testing and problem resolution.

2.38 Since completion of the fieldwork, Health advised that the Quality Framework, once implemented, would identify a minimum set of system documentation that is required for all new applications. The configuration management activity of the quality process will ensure that each of those deliverables is produced and reviewed as part of the signoff for each phase. Future releases of a system will be subject to the same quality controls, so that documentation will always be current, correct and relevant.

Quality assurance reviews and reporting

2.39 With the exception of the SIME application, the ANAO found that quality assurance reviews are generally not conducted. The practices of individual IT teams provide some assurance on the quality of the system, but not in a manner consistent with an integrated department-wide quality assurance program.

2.40 Since completion of the fieldwork, Health advised that formal review of project deliverables would be a key component of the Quality Framework. A draft of the IT Quality Framework was released for comment in March 2002 and from April 2002 the framework has been applied to all system development projects undertaken in the Department. The Framework mandates the review of all key project deliverables.

Development of a quality assurance knowledge base

2.41 The ANAO found that Health did not have a quality assurance knowledge base. A knowledge base contains longitudinal and comparative data on the performance of IT. It can be used as a reference tool for qualitative and quantitative data to assist with continuous improvement of IT within the department. Setting measures for the success of developments, and using those measures as the basis for evaluating both the success and the quality of the development, may facilitate development of a knowledge base. Over time, a reference tool could be created for Health’s internal benchmarking that would allow assessment of whether quality goals have been, and are being, achieved.

2.42 Since completion of the fieldwork, Health advised that the Quality Management Framework has as one of its key components the conduct of post-implementation reviews to evaluate the efficacy of the processes. An outcome of those reviews will be the maintenance of a knowledge base to which IT staff can refer for information of similar projects and to assist with the development of projects estimates, selection of tools and other information relating to the success (or otherwise) of the project. The Framework was scheduled for implementation in April 2002.

Benchmarking against norms

2.43 Health conducts no internal benchmarking of its management of IT or implementation of IT initiatives. In addition, Health did not benchmark against the IT industry generally, or against similar Commonwealth agencies.

2.44 Following the audit, Health advised that part of its proposed Quality Management Framework is to conduct internal and external benchmarking and continuous improvement activities. The BSB’s membership of the Australian

Software Metrics Association, and access to the resources of the International Software Benchmarking Standards Group's data repository will facilitate those activities.

Summary of main findings

2.45 The ANAO found that overall the SPARC and ORAC applications data tested during this audit exhibit quality characteristics. The data was found to be accurate, complete and consistent and reflected source documents. Testing confirmed payments made from these applications were appropriately certified and authorised. Minor improvement opportunities were noted in order to maintain and / or strengthen application data quality.

2.46 However, the SIME-1 development was running approximately 18 months behind schedule for one of the major phases. Delays have resulted in the lost opportunity for TGA staff to work on other projects and in the TGA realising the benefits of the new system according to the original schedule. Recognising the project was not progressing according to the original target, the TGA put in place processes to rectify and / or manage the delays. The TGA also accepted a revised implementation date with the intention of ensuring full value from the project would be realised.

2.47 The ANAO further found that, at the time of the audit, Health had not established at the departmental level an overarching quality culture or implemented a systematic framework of quality control responsibilities and practices, including quality assurance reviews. Health was not consistently applying system development methodologies and programming standards. The absence of a department-wide quality framework limits Health's ability to ensure IT investment decisions adhere to the requirements of quality standards, and that information produced through IT initiatives continue to meet the business needs.

2.48 The ANAO found that Health did not have a quality assurance knowledge base. A knowledge base contains longitudinal and comparative data on the performance of IT. It can be used as a reference tool for qualitative and quantitative data to assist with continuous improvement of IT within the department. Setting measures for the success of developments, and using those measures as the basis for evaluating both the success and the quality of the development, may facilitate development of such a knowledge base. Over time, a reference tool can be created for Health's internal benchmarking that would allow assessment of whether quality goals have been, and are being, achieved.

2.49 During fieldwork the ANAO found that Health conducts no regular internal benchmarking of its management of IT or implementation of IT initiatives. Health did not benchmark against the IT industry generally, or against similar Commonwealth agencies. Internal benchmarking allows an organisation to identify better practices internally; external benchmarking allows the organisation to compare its efficiency and effectiveness against other organisations, and identify improvement opportunities.

2.50 The ANAO noted that Health's *IT Strategic Review* identified the need to establish a quality framework. The ANAO acknowledges that Health was in the process of developing department-wide processes by which the overall quality of business information produced through IT initiatives can be assessed. Subsequent to the findings of the *IT Strategic Review*, Health was developing a framework of quality policies and standards to guide IT development efforts.

2.51 In managing quality for the SPARC and ORAC applications, the ANAO suggests that as part of proposed redevelopment efforts, Health consider:

- revision of post-implementation review procedures and the timing of such reviews to ensure an effective process of detecting and resolving errors;
- revising user and systems documentation to provide a current, central source of reference and training for user and technical staff; and
- use of automated controls to prevent automatic payments for closed residential aged care facilities (SPARC) or without submission of periodic financial statements (ORAC).

Recommendation

2.52 A recommendation in relation to setting and meeting timetables for IT quality management initiatives currently in progress is included at the end of Chapter 5.

3. Managing IT Service Levels

This Chapter discusses the levels of service delivered, and agreements for services provided by the Business Systems Branch to system owners in Health's divisions. Service level agreements and arrangements between Health and IBM–GSA, and between Health and Centrelink were outside the scope of this audit and were not considered. The Chapter also reports the results of the ANAO's testing of SPARC and ORAC to determine whether they met service delivery requirements.

Service level agreements

3.1 Service levels formalise the performance criteria against which the quantity and quality of service will be measured. The performance criteria enable management to identify the areas of under or non-performance and the achievement of service delivery targets. They facilitate timely management intervention and enable corrective actions to be undertaken.

3.2 A Service Level Agreement (SLA) states the responsibilities of a service provider, the rights of the system's users, and any penalties, if appropriate, for failure to meet the obligations defined in the agreement. This audit considered the service level arrangements between the BSB and the divisions to which it provides services, that is, the arrangements examined are internal to Health rather than with external service providers.

3.3 SLAs can be used to manage the expectations of both service provider and service user by creating a common understanding of the services to be provided, service volumes, priorities, needs, and responsibilities. The SLA can also define how services are monitored, and the measures to be used in monitoring. A SLA is a communications tool, a conflict prevention tool, and an objective basis for measuring service effectiveness. Appendix 3 includes the CobiT definition, along with specific control objectives, critical success factors, key performance indicators and key goal indicators, for *Define and Manage Service Levels.*

Audit approach

3.4 The ANAO tested service levels for the selected applications, including the existence / validity of internal service delivery performance measures; operating availability and performance statistics; change request turnaround periods; and the timeliness of processing and output distribution.

3.5 In addition, the following CobiT principles for define and manage service levels were considered[18]:

- *formal agreements;*
- *definition of responsibilities, response times and volumes, and charging;*
- *integrity guarantees and customer satisfaction; and*
- *cost/benefit analysis of required services levels.*

3.6 In coming to a view on the principal issues of defining and managing service levels, the ANAO sought to determine if service delivery parameters had been established between the BSB and owners of the three business applications included in this audit.

Service levels at Health

3.7 Responsibility for IT at Health is devolved. Divisional heads own and are responsible for their divisions' IT systems. They are also responsible for their own IT strategic planning. The BSB provides programming and other IT support services to divisions and, as mentioned earlier, it operates on a cost recovery basis for those services. While devolved responsibility enables divisions to have more direct control over IT activities, there is a need to ensure the approach is consistent and integrated with Health's overall IT strategic objectives.

3.8 At the time of the audit, Health did not have internal service level arrangements in place. However, it did have an external service level agreement with IBM-GSA, and a service level arrangement with Centrelink. Health's contract with IBM-GSA defines the service levels it requires from that firm. The Health / IBM-GSA service level agreement was outside the scope of this audit as the audit focused on agreements internal to Health, more specifically to any agreements between the BSB and the owners of Health's systems.

3.9 The arrangement with Centrelink defines how Health and Centrelink work together to design and deliver information, products and services to the Australian community arising from the Government's Health and Ageing policies. The arrangement defines the services each agency will provide, financial and performance monitoring requirements, and other procedures and mechanisms for the agreement's operation. The Health-Centrelink arrangement was also not included in the scope of the audit.

[18] Audit Guidelines, CobiT, 3rd Ed., July 2000, IT Process DS1: *'Define and Manage Service Levels' (Delivery and Support),* p. 124.

Audit findings

Applications testing

3.10 The ANAO examined and tested the SPARC and ORAC applications to identify if service delivery requirements had been established either at the departmental or operational levels, and the extent to which they met these requirements. The SIME development was not included in this testing.

3.11 The ANAO did not find that, at the department-wide level, Health had established specific service delivery targets through the implementation of internal service performance measures and service level agreements. However, the BSB did provide divisions with regular status reports of IT activity for their area of responsibility.

3.12 In spite of the absence of department-wide service delivery targets, testing conducted by the ANAO confirmed that the SPARC and ORAC systems are operating and being maintained within operational requirements. These requirements are defined, for example, in:

- the *Financial Management and Accountability Act 1997*;
- the *Chief Executive Instructions*;
- the *Aged Care Act 1997* and the *Residential Care Manual;* and
- funding agreements with indigenous health services.

3.13 ANAO's testing of a sample of payments from the SPARC and ORAC systems found those payments to be appropriately authorised and accurate, paid in a timely manner, and made in accordance with the defined operational requirements.

Formal agreements

3.14 The ANAO found that, at the time of audit, while a cost recovery mechanism was in operation:

- no documented SLA was in place between the ORAC system owner and the BSB to define the respective roles and responsibilities, and the required levels of service, support, and performance;
- a memorandum of understanding was being drafted between SPARC system owners and the BSB (as a precursor to a service agreement); and
- Health had yet to finalise maintenance arrangements for the SIME system and any ongoing involvement of the BSB.

3.15 Health did not have internal service level agreements between the BSB and system owners. However, there are agreements, on a project by project basis, that recognise the different responsibilities for managing IT service levels, project deliverables, time frames, and cost estimates. Following from a recommendation of the Corporate Activities Review, Health was in the process of developing internal service level arrangements, and the management and reporting of internal service level expectations. A Compact is being developed between Corporate Services Division and each of its client divisions to define at a higher level the generic responsibilities and services that Corporate Services Division will deliver. An attachment to the Compact will set out the services to be delivered by the BSB including service levels, operating arrangements, charging arrangements, and the responsibilities of the division owning the system. A document defining the roles and responsibilities for services is currently being discussed with Divisions.

Definition of responsibilities

3.16 The ANAO found that, while there were no documented definitions of responsibilities for the BSB and system owners, there are practices that recognise the different responsibilities for managing service levels. These practices include weekly team meetings and status reports. The process of defining responsibilities ensures the service obligations of each party are clearly understood. As indicated previously, formal arrangements are now being developed.

3.17 The ANAO found that technical matters, such as computer, network and help desk response times, are defined in the Health / IBM-GSA contract and are monitored by the Contestability Branch. It would be appropriate, however, for internal service agreements to specify the response times expected of the BSB in making priority and routine changes to systems. It would also be appropriate for the expected volume of work to be specified and actions to address variations from the expected volumes to be included.

3.18 Health advised the ANAO that the BSB Help Desk is a second level support service, receiving fault reports directly from the IBM-GSA Help Desk. It assigns all problems to the appropriate BSB resolution group within 24 hours of receipt from IBM-GSA. However, the priority of fault resolution and the implementation of system enhancements is determined by each individual system manager. Since the resources of the BSB are fully charged back to the client divisions, the priority of such activity is at the discretion and direction of the system managers. These arrangements will be more formally set out in the proposed CSD Compact.

3.19 The BSB charges divisions for its services on a cost recovery basis. Annual estimates for budgetary purposes are provided to divisions, and, as indicated above, a statement of work, on a project-by-project basis, estimates the cost of the BSB’s services for the project.

Integrity guarantees/Customer satisfaction

3.20 Any assurance on the integrity of a project deliverable will depend on the quality of the deliverable. Quality is assured by a consistent, planned and enforceable quality assurance process. Such a process did not exist at the departmental level within Health at the time of the audit. Quality assurance of IT initiatives is discussed in the previous chapter of this report.

3.21 The ANAO found that Health did not have a prescribed process in place to establish and assess the criteria upon which customer satisfaction could be measured. However, the practice of performing post-implementation reviews for application changes did ensure any significant problems are identified and resolved.

Cost-benefit analysis of required services

3.22 Health had implemented a structured process for the approval and funding of all significant IT initiatives. This process requires all developments and major changes to systems to be supported by a business case, including cost-benefit analyses for presentation to the ITC.

Summary of main findings

3.23 The SPARC and ORAC systems are operating and being maintained within operational requirements, despite the absence of department-wide defined internal service delivery performance measures. The SIME development was not tested. Processing with these applications was timely and accurate, and in accordance with the general business rules outlined in key legislation and Health policies.

3.24 At the departmental level, Health did not routinely use internal service delivery targets or service level agreements to define and prescribe the quantity and quality of service delivery. The ANAO found that, while there were no documented definitions of responsibilities between the Business Systems Branch and system owners, there are practices and agreements, on a project by project basis, that recognise the different responsibilities for managing IT service levels, project deliverables, time frames, and cost estimates. Following from a recommendation of the Corporate Activities Review, Health was in the process of developing internal service level arrangements, and the management and reporting of internal service level expectations.

3.25 Any assurance on the integrity of a project deliverable will depend on the quality of the deliverable. Quality is assured by a consistent, planned and enforceable quality assurance process. Such a process did not exist at the departmental level within Health at the time of the audit.

3.26 The ANAO found that Health did not have a prescribed process in place to establish and assess the criteria upon which customer satisfaction could be measured.

Recommendation

3.27 A recommendation in relation to setting and meeting timetables for IT service delivery initiatives currently in progress is included at the end of Chapter 5.

4. IT Systems Security

This Chapter examines Health's policies, practices and procedures to protect information resources. It reports the results of an evaluation of current security measures. It also identifies and reports the results of the testing of controls over information system security.

Systems security

4.1 Information is an important asset in any organisation. Like other assets, the protection and security of information is a primary management consideration. The Commonwealth's *Protective Security Manual* requires each agency to create and maintain appropriate security to protect its functions and resources. Therefore, it is necessary for controls and procedures to be implemented that achieve and maintain effective security. Appendix 4 includes the CobiT definition, along with specific control objectives, critical success factors, key performance indicators and key goal indicators, for *Ensure Systems Security*.

Audit approach

4.2 The ANAO included testing of security management for the selected applications, including data input and transaction authorisation procedures; logical security controls and procedures; and verifying the existence and completeness of transaction audit trails.

4.3 In addition, the following CobiT principles for ensure systems security were considered[19]:

- *confidentiality and privacy requirements;*
- *authorisation, authentication and access control;*
- *need-to-have and need-to-know; and*
- *incident handling, reporting and follow-up.*

4.4 In coming to a view on the principal issues of ensuring systems security, the ANAO sought to determine the existence or otherwise of:

- Health's policies and procedures for system security and access;
- documents and/or reports of IT security activities including, but not limited to, internal audit reports, user reports and any other assessments of Health's security management of IT resources;

[19] Audit Guidelines, CobiT, 3rd Ed., July 2000, IT Process DS5: *'Ensure Systems Security' (Delivery and Support),* p. 144.

- the currency of application security plans;
- tools or procedures used for monitoring security compliance, breaches and reporting;
- centralised security responsibilities; and
- user account management and logical access control mechanisms.

4.5 This audit did not examine Health's security over its use of the Internet. This aspect of Health's IT security environment had been examined and reported upon in 2000–01 by the ANAO[20].

IT security at Health

Commonwealth policy/Industry standards/Legislation

4.6 Commonwealth agencies must adhere to the security requirements, identified in the following:

- *Protective Security Manual (PSM)*. Commonwealth security policy is detailed in the PSM. All agencies must meet their security obligations under the PSM and must report annually to the Attorney-General's Department on their compliance;
- *AS/NZS 4444: Information Security Management*. The standard provides a specification for information security management systems, and it provides guidance for those who are responsible for initiating, implementing or maintaining security. It is intended to provide a common basis for developing organisational security standards and effective security management practice;
- *Australian Communications-Electronic Security Instructions 33 (ACSI33)*. These instructions provide guidance to agencies wishing to protect their information systems and are consistent with the PSM and AS / NZS 4444; and
- *Privacy Act 1998*. The legislation prescribes mandatory requirements for the manner, purpose and limits of data collection, as well as for the storage, security, access and disclosure requirements of personal information.

[20] ANAO Audit Report No.13, 2001–2002, *Internet Security within Commonwealth Government Agencies,* Canberra, December 2001.

Health's policies

4.7 Health had developed policies and procedures to support implementation and management of security requirements, including:

- *the Department Security Manual*. The manual had been produced in line with the requirements of the PSM and it encompasses departmental policy relating to protective security needs;
- *the Information Technology and Telecommunications (IT&T) Security Policy*. The policy had been developed to protect information assets from either accidental or deliberate harm through unauthorised access, disclosure, modification, manipulation or destruction. The aim of this policy is to assist Health to implement and maintain systems that have a high degree of integrity, availability and confidentiality;
- *Chief Executive Instructions (CEIs) and Procedural Guidelines, specifically:*

  a) *Ensuring the Integrity of Computer Systems*. As part of design, development or acquisition projects, the unit head must ensure control objectives are defined and a system control framework is set up to ensure that the level of risk associated with the system is reduced to a level that is considered appropriate to the situation.

  b) *Information Technology & Telecommunications (IT&T) Security*. A viable, independent, efficient and effective systems security function is required to be established and maintained to provide services to the whole of Health. The systems security function is to be undertaken in a manner consistent with the IT&T Security Policy, as set out in the PSM and technical advice obtained from the Defence Signals Directorate.

4.8 IT security management at Health is the responsibility of Health and a joint activity of the Contestability Branch and IBM-GSA. IBM-GSA manages logical security for access to the mainframe and network. The Contestability Branch reviews the security plans required for each system and monitors audit logs for servers, the mainframe, e-mail and Internet access.

4.9 As prescribed in the CEIs, relevant officers are required to ensure that, as part of design, development or acquisition projects for systems under their control, a system control framework is set up and control objectives are defined. Relevant officers are required to demonstrate compliance with the *Department Security Manual (DSM)*. This requirement ensures that measures are implemented to prevent unauthorised disclosure of information, to provide audit trails, and to protect data against unauthorised change.

Audit findings

Applications testing

User identification

4.10 The ANAO found that, overall, Health's security mechanisms are effective in managing and controlling access to IT application systems. Implemented mechanisms include the identification, authorisation and authentication of users, the definition and protection of resources (programs, applications and data), an independent security administration function, and logging / reporting of access attempts and violations.

4.11 Each authorised user has a security profile that implements the access control requirements of Health. The profile is a combination of a unique user-id, password, and access rights to computer resources. Regular review of these security profiles reduces the risk of unauthorised or inappropriate access to system resources.

4.12 The ANAO found that a regular review process was in place to ensure removal of redundant user-ids and access capabilities. In addition, a process for re-validation of user-ids had been established. The ANAO found that the access rights for business users to the SPARC system are reviewed quarterly. The ANAO considers the quarterly review of business users appropriate and an example of sound security practice.

4.13 The ANAO tested security profiles for SPARC and ORAC users and found the security framework to be satisfactory. Authorisation procedures, segregation of duties and timeliness of access profiles were confirmed and no issues were identified. Being under development, security for the SIME application was not tested.

Security plans

4.14 Health policy requires a system security plan to be developed and maintained for each application system. This is an example of good practice. There is a further requirement for the plan to be amended if changes are made to the underlying application system. As the requirement to develop security plans was a relatively recent initiative, plans are being developed retrospectively for all Health's application systems as time and resources allow. Considerable time will be required to complete this activity.

4.15 The ANAO found that, at the time of audit, the SPARC and ORAC Security Plans were not signed off, which was not consistent with Health policy. During the course of the audit, Health took action to finalise the security plans. The security plan for SIME was found to be extensive in its coverage. Without a comprehensive and up-to-date security plan for all applications, Health runs the risk of security breaches and performance deficiencies.

Confidentiality and privacy requirements

4.16 Because of the nature of the data collected, held and processed within Health's IT systems, the confidentiality and privacy of information are important business issues. Effective security controls help ensure confidentiality and privacy of data.

4.17 As part of its IT governance arrangements, Health had established two IT security related committees:

- *Information Planning and Privacy Committee (IPPC).* The Committee had the role of managing information within Health through identification of policy and future information needs, and the means to meet those needs. As the IPPC is primarily concerned with provision of strategic direction and guidance on information issues (i.e. data and supply of information and how information is held within Health), its role includes '*highlighting emerging information and privacy issues*…' (The 'IT Governance' section of this report discusses the role of the IPPC).

- *Department Protective Security Committee.* The Committee had the role of developing, approving, disseminating and coordinating integrated departmental security policies, standards and procedures to ensure that people, information and assets are protected against unacceptable risk. A primary objective of this Committee is to ensure that arrangements are in place to comply with the provisions of the PSM.

4.18 Although designated responsibility for privacy matters, at the commencement of this audit the IPPC had not developed policy or guidelines to ensure compliance with the information privacy principles of the Privacy Act. Since that time the IPPC has allocated a task to a subcommittee to address privacy issues with a completion date of July 2002. This subcommittee is currently reviewing personal data holdings. The ANAO also found that the Contestability Branch did not assess IT privacy issues as part of its review of application security plans.

4.19 The ANAO's review of application security plans indicates that information privacy requirements have not been adequately addressed as none of the plans reviewed had considered privacy issues.

4.20 In accordance with generally accepted control practices, Health's IT Security policy states, '*Systems development staff shall be isolated as much as possible* *from production data and the implementation of production system changes'*. In the systems reviewed, the ANAO found an instance of production data being used in test databases. While the use of production data in test databases may enable more effective testing, it increases the risk of unauthorised access to personal data, potentially circumventing privacy requirements. Actual personal data holdings must be afforded the same level of protection regardless of where they are held. The ANAO considers that, where technically practical, the risk could be minimised by altering / removing personal information from the records before using the data in a test environment.

4.21 In the situation identified it was not technically possible to alter the data, however since completion of the fieldwork, Health has ensured appropriate access and output controls were implemented to address the ANAO's concerns.

Authorisation, authentication and access control

4.22 Health relies on IT systems to collect, process, store and communicate information to meet its key business functions. Health's CEIs require a viable, independent, efficient and effective systems security function to be established and maintained in order to protect information.

4.23 The ANAO found that an IT&T Security Policy had been established by Health in order to implement and manage its security requirements. The policy assists achievement of security objectives through the use of IT systems that have a high degree of integrity, availability and confidentiality. This policy defines the responsibilities of system owners, administrators, authorised users, and security access controls. In addition, the policy addresses data, software, hardware, and communications security.

Need-to-have and Need-to-know

4.24 The IT&T Security Policy states, '*Access to information should be authorised according to the principles of "Need-to-Know" and "Least Possible Privilege"*'. Only authorised users with a need to view or use data should be granted access and they should be given only the minimum privileges needed to carry out their duties. Current control practices adhere to these principles.

4.25 Security plans are the commitment by the system owner to implement adequate measures to avoid, eliminate or reduce risks to an information system, including access risks. The creation and maintenance of the security plan is part of a risk management process to address security issues. The system security plan is a valuable method to define the required security measures, to monitor whether the prescribed solutions are implemented, and for future reference to ensure existing solutions can meet new threats.

Incident handling, reporting and follow-up

4.26 The ANAO found that the Contestability Branch monitors audit logs for potential breaches of security. Where breaches appear to have occurred, an explanation is requested of the relevant officer. Where usage is inappropriate, the Branch head is advised. Health prosecutes serious breaches, specifically incidents of fraud.

4.27 Good management practices include the recording, maintenance and review of key transactions and processing events. The ANAO found both the SPARC and ORAC applications maintain internal audit trails that enable analysis and tracking of transaction processing.

Summary of main findings

4.28 Health effectively manages its IT security, with appropriate security controls and compliance/monitoring procedures having been implemented. The maintenance of an appropriate security environment is an essential departmental activity given the importance of preserving the confidentiality and privacy of data holdings within Health. At the application level, the ANAO assessed segregation of duties, access controls, and authorisations, and found these to be effective.

4.29 Subsequent to completion of the audit fieldwork, the ANAO has conducted additional IT security and disaster recovery testing as part of the financial statement audit process. No issues were identified. At the departmental level good levels of security awareness exist and responsibilities for IT security are clearly assigned, managed and enforced.

4.30 The ANAO found that an IT&T Security Policy had been established by Health in order to implement and manage its security requirements. The Contestability Branch monitors audit logs for potential breaches of security. Where breaches appear to have occurred, an explanation is requested of the relevant officer. Where usage is inappropriate, the Branch head is advised. Health's policy provides for prosecution in serious breaches, specifically incidents of fraud.

4.31 Health's policy requires a system security plan to be developed and maintained for each application system. This is an example of good practice. There is a further requirement for the plan to be amended if changes are made to the underlying application system. The ANAO found that the SPARC and ORAC Security Plans were not signed off, but during the course of the audit Health took action to finalise the plans. The security plan for SIME was found to be very extensive in its coverage.

4.32 Because of the nature of the data collected, held and processed within Health's IT systems, the confidentiality and privacy of information are important business issues. Although designated responsibility for privacy matters, at the commencement of this audit the Information Planning and Privacy Committee (IPPC) had not developed policy or guidelines to ensure compliance with the information privacy principles of the Privacy Act. Since that time the IPPC has allocated a task to a subcommittee to consider privacy compliance issues. The subcommittee expects to report, by end July 2002, on information privacy principles requirements and departmental compliance, as a first step in the development of privacy policy and guidelines by December 2002.

4.33 The ANAO's review of application security plans indicates that information privacy requirements have not been adequately addressed as none of the plans reviewed had considered privacy issues.

4.34 Improvement opportunities were identified in the content and timeliness of completion of individual system security plans, and in the practice of using production data (that contains personal information) for testing purposes. Some plans may need revising to address privacy concerns identified by the Information Planning and Privacy Committee work program.

Recommendation No.1

4.35 The ANAO recommends that Health:

- review the content of all application security plans, using the SIME security plan as an example of sound practice, to ensure Health's security requirements have been fully addressed;
- include privacy requirements in security plans (where appropriate); and
- ensure that for any production data used in test environments, the data does not include identifiable personal information.

Health's Response

4.36 Point 1—Agreed. Over the next 12 months the Department will review all application Systems Security Plans to ensure their currency and completeness.

4.37 Point 2—Agreed. The Department will endeavour to ensure the privacy requirements are fully addressed in the Systems Security Plans.

4.38 Point 3—Agreed. However, business requirements have dictated the requirement to use real data in the test environments. In these cases the Department has taken a risk management approach and put in place strict security procedures and processes that are commensurate with the full production environment. All these processes are being addressed in the relevant Security Plans as part of the Threat and Risk Assessment.

5. Monitoring IT Processes

This Chapter examines the activities that management had implemented to monitor key IT processes. It reports the results of monitoring practices both overall and for selected applications.

Monitoring IT

5.1 Management must ensure that an internal control system or framework is in place that supports business processes. The purpose is to confirm that IT processes are aligned with the IT strategy and the business goals.

5.2 All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. Monitoring activities address management's oversight of the organisation's control process. Appendix 5 includes the CobiT definition, along with specific control objectives, critical success factors, key performance indicators and key goal indicators, for *Monitor the Processes*.

Audit approach

5.3 The ANAO tested the monitoring processes for the selected applications, including whether monitoring covers all appropriate aspects of the systems; validating the accuracy of data extracted for inclusion in management reports; and verifying that reports are considered and acted upon.

5.4 In addition, the following CobiT principles for monitoring the (IT) processes were considered[21]:

- *scorecards with performance drivers and outcome measures;*
- *customer satisfaction assessments;*
- *management reporting;*
- *knowledge base of historical performance;*
- *external benchmarking; and*
- *involvement of audit.*

5.5 In coming to a view on the principal issues of monitoring the processes, the ANAO sought to determine the existence or otherwise of:

[21] Audit Guidelines, CobiT, 3rd Ed., July 2000, IT Process M1: *'Monitor the Processes' (Monitoring)* p. 194.

- policies and procedures relating to monitoring and reporting on IT performance;
- documents and / or reports of IT activities including, but not limited to, internal audit reports, user reports, user satisfaction surveys, committee minutes and any other assessments of Health's use of IT resources;
- key performance indicators and / or critical success factors used to measure IT performance;
- data used for monitoring IT resources and the appropriateness of the data collected; and
- the existence and timeliness of IT performance management review processes.

Monitoring of IT at Health

5.6 The ANAO found that Health had a number of mechanisms for monitoring IT performance. These mechanisms include the oversight roles of the Audit, ITC, and IPPC committees:

- as part of the audit reporting mechanism, internal and external reports are provided to the Audit Committee. The Committee had responsibility for ensuring action is taken on all recommendations raised in these reports. IT issues raised are addressed as part of this process;
- the ITC considers and makes decisions on business proposals for new IT systems or major changes to existing systems. The ITC also monitors the progress of developments; and
- the IPPC role relates to matters of information management and privacy.

5.7 Additionally at the application level, there are various divisional management committees, including steering and change committees, which approve and monitor all activities undertaken. These committees perform a valuable oversight role.

Audit findings

Application testing

SPARC application: Management reporting

5.8 The ANAO found that management's reporting requirements for assuring the accuracy, completeness, consistency and currency of SPARC data were met from two sources, SPARC standard reports and the Aged and Community Care

Management Information System (ACCMIS). These sources enable the effectiveness of SPARC processing to be assessed.

5.9 However, there was an absence of a department-wide requirement for the specification and subsequent monitoring of key goal indicators, key performance indicators and critical success factors for applications. This absence limits Health's ability to assess and report on the efficiency and economy of SPARC processing.

5.10 SPARC reporting is restricted to a number of structured reports and the application does not easily accommodate direct query facilities. The lack of unplanned reporting is partially met by ACCMIS. The Aged and Community Care Division developed ACCMIS as a central data repository for the Division's operational computer systems. The need for ACCMIS was driven by the absence of integrated reporting and analysis facilities within divisional systems. ACCMIS is used for program and policy development, planning, ad-hoc queries and reporting on business opportunities and service standards. Consequently, the accuracy of data holdings within ACCMIS is an important business requirement. The ANAO compared key elements of ACCMIS data against source data held within SPARC, and found that ACCMIS data accurately reflected SPARC data.

5.11 The ANAO tested payments made through SPARC over an 18-month period ending December 2001. The payments were found to be correctly calculated and appropriately authorised. Through its analysis of over 40 000 payment transactions, the ANAO identified a small number of potential overpayments relating to advance payments made to residential care facilities after they had co-located or closed. Further ANAO testing and analysis confirmed only two advance payments had been made where recovery action had not been initiated. Health immediately initiated recovery on these payments.

5.12 During the entry and processing of claims, SPARC had the capacity to detect potential data discrepancies, such as dates outside parameters or exception to operational requirements. These discrepancies are identified and reported to the claimant for action. This in-built error detection within SPARC is a good control feature that assists in ensuring only correct payments are processed.

5.13 A program of visits to residential care facilities premises is performed to ensure that the facility maintains a satisfactory level of service and facilities. The Division receives monitoring information from these visits for entry into SPARC. The ANAO found that monitoring and compliance activities contribute to the reliability of data submitted by care facilities.

5.14 The ANAO noted that a project proposal had been produced to support redevelopment of residential aged care systems (predominantly SPARC) in order to implement an electronic commerce environment, including electronic claims processing, in line with Commonwealth e-commerce initiatives. The overall objective is to deliver administrative efficiencies and lower transaction costs.

ORAC application: Management reporting

5.15 The ORAC system data was monitored for accuracy, completeness, consistency and currency. However, as with the SPARC application, key goal indicators, key performance indicators and critical success factors are not used to report on ORAC's efficiency and economy.

5.16 The ANAO found monitoring of ORAC processing was facilitated by the existence of an audit trail of system activity. The audit trail includes identification of the individual taking action and the dates the actions were executed.

5.17 A program of operational audits is performed to ensure that indigenous health services are in compliance with their funding agreements with Health.

5.18 The ANAO noted that a project proposal has been produced to support the development of a system to manage the entire Office of Aboriginal and Torres Strait Islander Health funding program. This development will provide e-commerce and workflow functionality, and investigate utilising a payment facility of the corporate financial management information system. This development is planned to replace ORAC in the near future.

SIME application: Management reporting

5.19 At completion of audit fieldwork, SIME was still in the development phase and processes for monitoring its operation were yet to be established. However, the establishment of appropriate monitoring processes was an identified project task.

5.20 The ANAO found that Health had appropriate monitoring mechanisms to oversee the development of SIME. Monitoring mechanisms included independent project management advice and independent quality assurance. The ANAO also found that key project performance measures were established at project initiation. These provide a base line for project reporting.

Scorecards

5.21 Health did not use scorecards to assess achievement of IT projects objectives. In any organisation, measurement of the success or failure of any project is determined by the setting of performance targets in the business case for the project, and measuring the result of the project against those targets (i.e. a scorecard). A requirement is that targets are appropriately mapped to the expected business outcomes. Measurement against targets allows for a picture of IT performance for decision-making and accountability purposes.

5.22 In line with the recommendations of the *IT Strategic Review*, Health advised it was currently in the process of developing policies and procedures for monitoring and reporting on IT performance. Health was also in the process of establishing performance targets for IT.

5.23 The ANAO found that post-implementation reviews were conducted or, in the case of SIME, planned, for developments or substantive changes to each of the systems examined. The reviews identified faults, improvements, opportunities and sound practice in the development/change processes.

5.24 As indicated earlier, Health advised the ANAO that its proposed measurement program would facilitate the setting of project measures and thus the setting of project targets. Targets will take into consideration industry data for defect rates and delivery productivity.

Customer satisfaction assessment

5.25 The ANAO found that financial and timeliness targets were set for significant changes to systems and for new system developments. Although important, these targets alone do not indicate the overall success of a project. Customer satisfaction, both within Health (the system users) and external to Health (e.g. residential care facilities and recipients of grants) is a major indicator of the success of IT systems. The ANAO found no surveys of internal or external users of the systems were performed.

Management reporting

5.26 This principle has been addressed earlier in the application testing section of this chapter (refer to paragraphs 5.8 to 5.20).

Knowledge base

5.27 This principle has been addressed earlier in the chapter on Managing Quality (refer to paragraphs 2.41 and 2.42).

External benchmarking

5.28 The ANAO found that Health did not engage in any benchmarking of its IT function against external organisations in order to assess the overall effectiveness of IT activities. Benchmarking enables an organisation to compare the implementation or management of their IT in terms of cost, timeframe, and suitability of product which may warrant further investigation; and highlight opportunities for business re-engineering, process improvement or alternate delivery options.

5.29 While not undertaking benchmarking, Health did use a standard industry measurement, function point analysis, to measure the size of its applications. This analysis provides an indication of the overall complexity of an application, and the resources required to develop and maintain the application.

Internal Audit

5.30 The ANAO found that Internal Audit had conducted a number of audits of aspects of IT in recent years. The audits are conducted internally or by contracting with private sector organisations to undertake and report on the findings. The ANAO also found that Health's Audit Committee appropriately considered the reports of the audits and ensured recommendations were addressed.

5.31 Internal Audit performs a significant role in providing objective and independent advice on the effectiveness, efficiency, economy, appropriateness, financial regularity, risk of fraud and waste, and legal compliance of Health's systems and programs, including an expert advisory role in IT systems development and controls.

5.32 Internal Audit's activities are generally addressed through Internal Audit representation on steering committees. Internal Audit considers one of its roles on the committees as ensuring quality assurance is a primary consideration in projects. However, overall responsibilities for quality assurance and for ensuring an appropriate control environment are established rests with each system owner.

Summary of main findings

5.33 At the operational level, Health effectively monitored the data of the SPARC and ORAC systems for accuracy, completeness, consistency, currency and uniqueness, and appropriate arrangements were in place to produce and review reports to management. As the SIME project was under development, monitoring procedures had not been developed, but this was an identified project task.

5.34 While operational monitoring of data was taking place, at the department-wide level Health did not routinely use key goal indicators, key performance indicators and critical success factors to measure and report on the efficiency and economy of IT processing. It did not have performance targets (scorecards) for IT, nor did it undertake customer satisfaction assessments.

5.35 As previously mentioned in the key findings for the chapter on Managing IT Quality, the ANAO found that Health did not engage in any benchmarking of its IT function against external organisations in order to assess the overall effectiveness of IT activities. Benchmarking is relevant to both quality and monitoring. However, Health did use a standard industry measurement, function point analysis, to measure the size of its applications.

5.36 In line with the recommendations of the *IT Strategic Review,* Health is developing policies and procedures for monitoring and reporting on IT performance. It is establishing performance targets for IT and implementing internal and external benchmarking.

5.37 The ANAO found that, at the operational level, financial and timeliness targets were set for significant changes to systems and for new system developments. Although important, these targets alone do not indicate the overall success of a change or development project. Customer satisfaction, both within Health (the system users) and external to Health (e.g. residential care facilities and recipients of grants) is a major indicator of the success of IT systems. The ANAO found no surveys of internal or external users of the systems were performed.

5.38 Internal Audit had conducted a number of audits of aspects of IT in recent years. Internal Audit's activities are generally addressed through Internal Audit representation on steering committees. Health's Audit Committee appropriately considered the reports of the audits and ensured recommendations were addressed.

Recommendation No.2

5.39 The recommendations of Health's *IT Strategic Review* provide a blueprint for improving overall IT management within the department. The ANAO recommends that Health set and meet a firm timetable for implementation of the Review's recommendations relating to:

- completion of the IT Quality Framework and system development methodologies;
- the development of service delivery targets and service level arrangements between BSB and client divisions; and
- developing a program for measuring and benchmarking the performance of its IT, including measures to assess the success or otherwise of IT projects.

Health's Response

5.40 Point 1—Agreed. While both the IT Quality Framework and the system development methodology (Project Lifecycle) are documents which will continually evolve with continuous improvement practices, from April 2002 they have been in use as the standard for business system development at Health.

5.41 Point 2—Agreed. Formal internal service level agreements are under consideration within the Department. A document defining the roles and responsibilities for services is being discussed with Divisions.

5.42 Point 3—Agreed. Subject to the availability of appropriate funding and resources, a measurement and benchmarking program is planned to commence during Q3 2002.

6. IT Governance

This Chapter discusses IT governance issues in Health, including the responsibilities of, and relationships between, governance committees. IT governance is the overarching structure that controls and links the IT processes, resources and information.

Governance

6.1 Agency governance is about how an organisation is managed, its corporate and operational structures, its culture, its policies and strategies, and the ways in which it deals with stakeholders. It is concerned with structures and processes for decision-making and with the controls and behaviour that support effective accountability for performance outcomes / results. Key components of corporate governance are business planning, internal controls including risk management, performance monitoring and accountability and relationships with stakeholders.

6.2 IT governance is an integral part of agency governance. IT governance ensures that the agency's IT strategy is aligned with and supports the agency business strategy, appropriate control structures are implemented, IT resources are used responsibly and IT performance is measured and appropriately managed. In summary, IT governance is a system of control that ensures that business objectives are achieved[22]. It is the mechanism that establishes an overarching framework within which all IT activities occur. Appendix 6 includes the CobiT definition, along with critical success factors, key performance indicators and key goal indicators, for *IT Governance*.

Audit approach

6.3 The following CobiT principles of IT governance were considered[23]:

- *responsibility for approving IT strategies, budgets and structures resides at board level (i.e. the Departmental Management Committee (DMC) in the case of Health) and IT is a regular item for discussion at board level;*
- *the management structures for IT are appropriate and effective; and*
- *the organisation's audit committee ensures that IT is included in the program of audits, reviews the results of audits and follows up on recommendations.*

[22] Audit Guidelines, CobiT, 3rd Ed., July 2000, p. 15.

[23] As mentioned in Chapter 1, the ANAO applied selected CobiT guidelines to assist with the assessment of the department's management and operation of IT.

6.4 In considering these issues, the ANAO focussed on those aspects of IT governance at Health that were most likely to have a significant impact upon the overall achievement of business objectives, specifically:

- the role of the DMC in relation to IT governance issues;
- the roles of and relationship between the Information Planning and Privacy Committee (IPPC) and the Information Technology Committee (ITC);
- responsibility for progressing the recommendations of the *IT Strategic Review;* and
- the internal audit work program.

IT governance at Health

6.5 The DMC is Health's key governance committee and primary decision-making forum, advising the Secretary on strategic policy and management matters. A network of major committees and forums supports the DMC. Two of the committees have responsibility for IT—the IPPC and the ITC:

- the IPPC is responsible for Health's key information and communication needs and strategies, the development and monitoring of Health's Information Management Plan, the Corporate Communication Strategy, and Health's approach to its privacy obligations; and
- the ITC is responsible for developing the long-term capital strategy for Health's IT requirements, identifying IT needs and priorities, the IT Strategic Plan, and assessing and monitoring Health's IT investments. The ITC allocates funds from the Capital Fund, as it considers appropriate. Each IT investment decision must be supported by a business case. The ITC considers the business case for new developments or significant changes to existing systems to ensure that those systems align with, and are consistent with, Health's existing and planned computer environment.

6.6 The memberships of the various governance committees within Health have broad representation from throughout the department. This representation has facilitated the identification and discussion of department-wide issues and areas of concern, as well as greatly enhancing communications between divisions.

6.7 Health had devolved responsibility for IT. There is no Chief Information Officer and divisions are responsible for developing their own IT strategies, including IT Strategic Plans for the division.

6.8 In addition to six other non-IT branches, the Corporate Services Division of Health contains two IT branches, the Business Systems Branch (BSB) and the Contestability Branch:

- the BSB provides programming and systems development expertise to divisions and operates on a cost recovery basis. Divisions can elect to utilise the BSB's services or source externally if there is valid business justification. In conjunction with IBM-GSA, the BSB is also responsible for managing changes to systems and infrastructure. At the time of the audit fieldwork, the BSB did not have a mandate to examine the quality of systems in development unless invited to do so by the system owners; and
- the Contestability Branch is responsible for managing the contract with Health's service provider, IBM-GSA. This Branch also had responsibility for IT security and providing the Secretariat for the ITC.

6.9 IT at Health had been the subject of significant change and review in recent years, including the outsourcing of its infrastructure to IBM-GSA and reviews by consultants. As previously mentioned, during 2000 Health commissioned an Information Technology Strategic Review (*IT Strategic Review*). The report from this review, released in mid-2001, detailed a number of areas for change in Health's management of IT. These areas included project management, performance management, requirements engineering and relationship management.

Audit findings

Departmental Management Committee

6.10 The ANAO found the DMC had allocated some of its IT governance activity to the IPPC and the ITC. The DMC, however, retains for itself overall responsibility for IT governance including decisions on strategic, financial and corporate management issues of portfolio significance, overseeing all major management strategies, and considering and endorsing strategic level plans across Health. The DMC endorsed the *IT Strategic Review* and allocated overall responsibility for implementation of the recommendations to the Business Improvement Committee. This latter Committee was examining corporate activities, including IT, for the whole of Health as part of the Corporate Activities Review.

Information Planning and Privacy Committee

6.11 A decision of the DMC in November 1997 created the IPPC in its present form. Its roles and responsibilities were extended in November 2000. At the commencement of the audit the role of the IPPC was being redefined by Health to better reflect its governance responsibilities. Since that time significant progress has been made in clarifying the role, responsibilities, and relationships of the IPPC. It has now developed a work plan that identifies its key focus areas, and it has established a number of subcommittees to address them. This Committee is responsible for Health's key information and communication needs and strategies, including development and monitoring of the Information Management Plan and Corporate Communications Strategy.

Information Technology Committee

6.12 The ANAO found that the ITC had a clear purpose and charter. The Committee plays a strategic governance role in centralising and controlling reinvestment in IT. The ITC considered business cases for proposed projects, and ensured that the plans aligned with overall Health IT priorities. The ITC approved or rejected IT proposals and, where appropriate, approved funding from the IT capital fund. A joint Health–IBM-GSA committee, responsible for implementing changes to systems, ensures proposals not approved by the ITC are not implemented.

ITC–IPPC relationship

6.13 The ITC and the IPPC share responsibilities for IT within Health. The IPPC had responsibility for developing the Information Management Plan whereas the ITC had responsibility for developing the IT Strategic Plan. There is an overlap of some elements between these two plans and Health had recognised the need to ensure cohesion between these plans. The IPPC and the ITC are working toward that goal.

IT management practices

6.14 The ANAO found that, at the time of the audit, Health had some unresolved department-wide IT governance issues that present risks to the continued management and operation of IT. These issues were identified during the *IT Strategic* Review and, at the completion of audit fieldwork, Health was yet to fully develop and implement responses to the recommendations of this review. The practices yet to be addressed, and which have been described in earlier chapters of this report, include:

- the establishment of an overarching IT quality framework;
- the adoption and implementation of an up-to-date system development methodology;
- the implementation of service delivery targets and service level agreements;

- the establishment of policies and practices to ensure that privacy issues are appropriately addressed; and
- the establishment of performance monitoring and benchmarking processes.

IT Strategic Review

6.15 The recommendations from the *IT Strategic Review* were endorsed by the DMC in late 2001, and the BSB had been allocated responsibility for implementing recommendations (by mid–2002) relating to strengthening the quality and efficiency of applications development processes. The Business Improvement Committee is monitoring overall implementation of all recommendations. Key activities of the BSB activity include:

- implementing a process model for applications development;
- strengthening capability in a number of areas, including requirements engineering and customer relations;
- strategic use of outsourcing;
- performance measurement; and
- implementing support systems, e.g. workflow and a standardised systems development methodology.

Internal audit work program

6.16 The ANAO found that Health had an Audit Committee which oversights the Internal Audit work program, reviews the results of internal and external audits, including IT audits, and ensures recommendations from audits are acted upon. The ANAO found IT reviews were included in the Internal Audit work program. The role of Internal Audit was previously discussed in Chapter 5 *Monitoring IT Processes.*

Summary of main findings

6.17 At the commencement of the audit, Health had yet to fully implement department-wide IT management practices that ensure consistency with accepted best practice and optimal use in the management and operation of IT. The ANAO found that Health had established IT governance committee structures during 2000 as an integral part of overall governance arrangements within the department.

6.18 Recognising the need to further revise IT governance, Health commissioned the *IT Strategic Review* in late 2000 to ensure that the department had the capability to satisfy current and future needs for information and services. The report from this review, released in mid-2001, identified a number areas of concern in terms of IT structures and processes, and made a number of recommendations to address these concerns. Health is in the process of addressing the recommendations.

Canberra ACT
18 July 2002

Ian McPhee
Acting Auditor-General

Appendices

Appendix 1

CobiT: Control Objectives for Information and Related Technology

CobiT Executive Overview[24]

Critically important to the survival and success of an organisation is effective management of information and related Information Technology (IT). In this global information society—where information travels through cyberspace without the constraints of time, distance and speed—this criticality arises from the:

- increasing dependence on information and the systems that deliver this information;
- increasing vulnerabilities and a wide spectrum of threats, such as cyber threats and information warfare;
- scale and cost of the current and future investments in information and information systems; and
- potential for technologies to dramatically change organisations and business practices, create new opportunities and reduce costs.

For many organisations, information and the technology that supports it represent the organisation's most valuable assets. Moreover, in today's very competitive and rapidly changing business environment, management has heightened expectations regarding IT delivery functions: management requires increased quality, functionality and ease of use; decreased delivery time; and continuously improving service levels-while demanding that this be accomplished at lower costs.

Many organisations recognise the potential benefits that technology can yield. Successful organisations, however, understand and manage the risks associated with implementing new technologies.

There are numerous changes in IT and its operating environment that emphasise the need to better manage IT-related risks. Dependence on electronic information and IT systems is essential to support critical business processes. In addition, the regulatory environment is mandating stricter control over information. This, in turn, is driven by increasing disclosures of information system disasters and

[24] This Executive Overview is taken from the CobiT Executive Summary. CobiT is copyright 1996, 1998, 2000 Information Systems Audit and Control Foundation. Reprinted with the permission of the Information Systems and Control Foundation and IT Governance Institute.

increasing electronic fraud. The management of IT-related risks is now being understood as a key part of enterprise governance.

Within enterprise governance, IT governance is becoming more and more prominent, and is defined as a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes. IT governance is integral to the success of enterprise governance by assuring efficient and effective measurable improvements in related enterprise processes. IT governance provides the structure that links IT processes, IT resources and information to enterprise strategies and objectives. Furthermore, IT governance integrates and institutionalises good (or best) practices of planning and organising, acquiring and implementing, delivering and supporting, and monitoring IT performance to ensure that the enterprise's information and related technology support its business objectives. IT governance thus enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage.

IT Governance

A structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes.

Organisations must satisfy the quality, fiduciary and security requirements for their information, as for all assets. Management must also optimise the use of available resources, including data, application systems, technology, facilities and people. To discharge these responsibilities, as well as to achieve its objectives, management must understand the status of its own IT systems and decide what security and control they should provide.

Control Objectives for Information and related Technology (CobiT), now in its 3rd edition, helps meet the multiple needs of management by bridging the gaps between business risks, control needs and technical issues. It provides good practices across a domain and process framework and presents activities in a manageable and logical structure. CobiT's 'good practices' means consensus of the experts-they will help optimise information investments and will provide a measure to be judged against when things do go wrong.

Management must ensure that an internal control system or framework is in place which supports the business processes, makes it clear how each individual control activity satisfies the information requirements and impacts the IT resources. Impact on IT resources is highlighted in the CobiT Framework together with the business requirements for effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability of information that need to be satisfied. Control, which includes policies, organisational structures, practices and procedures, is management's responsibility. Management, through its enterprise governance, must ensure that due diligence is exercised by all individuals involved in the management, use, design, development, maintenance or operation of information systems. An IT control objective is a statement of the desired result or purpose to be achieved by implementing control procedures within a particular IT activity.

Business orientation is the main theme of CobiT. It is designed to be employed not only by users and auditors, but also, and more importantly, as comprehensive guidance for management and business process owners. Increasingly, business practice involves the full empowerment of business process owners so they have total responsibility for all aspects of the business process. In particular, this includes providing adequate controls.

The CobiT Framework provides a tool for the business process owner that facilitates the discharge of this responsibility. The Framework starts from a simple and pragmatic premise:

In order to provide the information that the organisation needs to achieve its objectives, IT resources need to be managed by a set of naturally grouped processes.

The Framework continues with a set of 34 high-level Control Objectives, one for each of the IT processes, grouped into four domains: planning and organisation, acquisition and implementation, delivery and support, and monitoring. This structure covers all aspects of information and the technology that supports it. By addressing these 34 high-level control objectives, the business process owner can ensure that an adequate control system is provided for the IT environment.

IT governance guidance is also provided in the CobiT Framework. IT governance provides the structure that links IT processes, IT resources and information to enterprise strategies and objectives. IT governance integrates optimal ways of planning and organising, acquiring and implementing, delivering and supporting, and monitoring IT performance. IT governance enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage.

In addition, corresponding to each of the 34 high-level control objectives is an Audit Guideline to enable the review of IT processes against CobiT's 318 recommended detailed control objectives to provide management assurance and / or advice for improvement.

Maturity Models

The Management Guidelines, CobiT's most recent development, further enhances and enables enterprise management to deal more effectively with the needs and requirements of IT governance. The guidelines are action oriented and generic and provide management direction for getting the enterprise's information and related processes under control, for monitoring achievement of organisational goals, for monitoring performance within each IT process and for benchmarking organisational achievement.

Specifically, CobiT provides Maturity Models for control over IT processes, so that management can map where the organisation is today, where it stands in relation to the best-in-class in its industry and to international standards and where the organisation wants to be; Critical Success Factors, which define the most important management-oriented implementation guidelines to achieve control over and within its IT processes; Key Goal Indicators, which define measures that tell management—after the fact—whether an IT process has achieved its business requirements; and Key Performance Indicators, which are lead indicators that define measures of how well the IT process is performing in enabling the goal to be reached.

CobiT's Management Guidelines are generic and action oriented for the purpose of answering the following types of management questions: How far should we go, and is the cost justified by the benefit? What are the indicators of good performance? What are the critical success factors? What are the risks of not achieving our objectives? What do others do? How do we measure and compare?

CobiT also contains an Implementation Tool Set that provides lessons learned from those organisations that quickly and successfully applied CobiT in their work environments. It has two particularly useful tools-Management Awareness Diagnostic and IT Control Diagnostic-to assist in analysing an organisation's IT control environment.

Over the next few years, the management of organisations will need to demonstrably attain increased levels of security and control. CobiT is a tool that allows managers to bridge the gap with respect to control requirements, technical issues and business risks and communicate that level of control to stakeholders. CobiT enables the development of clear policy and good practice for IT control throughout organisations, worldwide. Thus, CobiT is designed to be the breakthrough IT governance tool that helps in understanding and managing the risks and benefits associated with information and related IT.

Appendix 2

Manage Quality: Definition, Controls and Measures

CobiT definition

CobiT defines control over managing quality in an IT environment:

> Control over the IT process **Manage Quality**, with the business goal of meeting the IT customer requirements, is enabled by the planning, implementing and maintaining of quality management standards and systems providing, for distinct development phases, clear deliverables and explicit responsibilities.[25]

According to CobiT, this control ensures delivery of information to the business that addresses the required information criteria (primarily, effectiveness, efficiency, and integrity) and is measured by key goal indicators. The control considers critical success factors that leverage specific IT resources and is measured by key performance indicators.

Controls

*The following control objectives are based on CobiT guidelines for **Manage Quality**. The control objectives were used by the ANAO in considering Health's management of IT quality. The guidelines are provided here for consideration by Health for inclusion in the development of its quality policies, plans and processes.*

General quality plan

Management should develop and regularly maintain an overall quality plan based on the organisational and IT long-range plans. The plan should promote the continuous improvement philosophy and answer the basic questions of what, who and how.

Quality assurance approach

Management should establish a standard approach regarding quality assurance that covers both general and project specific quality assurance activities. The approach should prescribe the type(s) of quality assurance activities (such as reviews, audits, inspections, etc.) to be performed to achieve the objectives of the general quality plan. It should also require specific quality assurance reviews.

[25] Management Guidelines, CobiT, 3rd Ed., July 2000, IT Process PO11: *'Manage Quality' (Planning and Organisation),* p. 44.

Quality assurance planning

Management should establish a standard approach regarding quality assurance that covers both general and project specific quality assurance activities. The approach should prescribe the type(s) of quality assurance activities (such as reviews, audits, inspections, etc.) to be performed to achieve the objectives of the general quality plan. It should also require specific quality assurance reviews.

Quality assurance review of adherence to IT standards and procedures

Management should ensure that the responsibilities assigned to the quality assurance personnel include a review of general adherence to IT standards and procedures.

System Development Life Cycle Methodology

The organisation's management should define and implement IT standards and adopt a system development life cycle methodology governing the process of developing, acquiring, implementing and maintaining computerised information systems and related technology. The chosen system development life cycle methodology should be appropriate for the systems to be developed, acquired, implemented and maintained.

System Development Life Cycle Methodology for major changes to existing technology

In the event of major changes to existing technology, management should ensure that a system development life cycle methodology is observed, as in the case of the acquisition or development of new technology.

Updating the System Development Life Cycle Methodology

Management should implement a periodic review of its system development life cycle methodology to ensure that its provisions reflect current generally accepted techniques and procedures.

Coordination and communication

Management should establish a process for ensuring close coordination and communication between customers of the IT function and system implementors. This process should entail structured methods using the system development life cycle methodology to ensure the provision of quality IT solutions which meet the business demands. Management should promote an organisation that is characterised by close cooperation and communication throughout the system development life cycle.

Third-party implementor relationships

Management should implement a process to ensure good working relationships with third-party implementors. Such a process should provide that the user and implementor agree to acceptance criteria, handling of changes, problems during development, user roles, facilities, tools, software, standards and procedures.

Program documentation standards

The organisation's system development life cycle methodology should incorporate standards for program documentation, which have been communicated to the concerned staff and enforced. The methodology should ensure that the documentation created during information system development or modification projects conforms to these standards.

Program testing standards

The organisation's system development life cycle methodology should provide standards covering test requirements, verification, documentation and retention for testing individual software units and aggregated programs created as part of every information system development or modification project.

System testing standards

The organisation's system development life cycle methodology should provide standards covering test requirements, verification, documentation and retention for the testing of the total system as a part of every information system development or modification project.

Parallel/pilot testing

The organisation's system development life cycle methodology should define the circumstances under which parallel or pilot testing of new and / or existing systems will be conducted.

System testing documentation

The organisation's system development life cycle methodology should provide, as part of every information system development, implementation or modification project, that the documented results of testing the system are retained.

Quality assurance evaluation of adherence to development standards

The organisation's quality assurance approach should require that a post-implementation review of an operational information system assess whether the project team adhered to the provisions of the system development life cycle methodology.

Quality assurance review of the achievement of IT objectives

The quality assurance approach should include a review of the extent to which particular systems and application development activities have achieved the objectives of the information services function.

Quality metrics

Management should define and use metrics to measure the results of activities, thus assessing whether quality goals have been achieved.

Reports of quality assurance reviews.

Reports of quality assurance reviews should be prepared and submitted to management of user departments and the IT function.

Measures

Critical Success Factors

CobiT outlines the critical success factors associated with manage quality.

- A clearly defined and agreed upon development process has been created to perform quality assurance.
- Quality is defined by the organisation with clear roles for the quality assurance processes and quality control procedures.
- A quality assurance program has been implemented with well-defined, measurable quality standards and quality control processes have been defined, resourced and aligned.
- There is continuous improvement and a defined knowledge base for processes and metrics.
- There is quality education and training program.
- Stakeholders are involved in the quality assurance program.

- A positive quality culture is consistently promoted by all layers of management.
- Awareness exists that quality standards should equally apply to processes and projects where reliance is placed on third-parties.
- Every delivery process needs to have proper quality assurance criteria.
- Emphasis is provided on training IT and end-user staff in testing methods and techniques.

Key Performance Indicators

CobiT outlines key performance indicators associated with manage quality.

- Number of IT processes and projects with active quality assurance management participation.
- Number of documented quality assurance monitoring and testing activities.
- Number of quality assurance peer reviews.
- Number of IT processes and projects that have been benchmarked.
- Number of meetings between stakeholders and developers.
- Average number of training days in quality management.
- Number of projects with documented and measured quality criteria.

Key Goal Indicators

CobiT outlines key goal indicators associated with manage quality.

- Number of IT processes and projects that satisfy stakeholder requirements.
- Increased rating for customer satisfaction with services rendered.
- Number of IT processes and projects formally signed off by quality assurance without significant rework.
- Decreased number of quality defects.
- Decreased number of non-compliance reports against quality standards.

Appendix 3

Define and Manage Service Levels: Definition, Controls and Measures

CobiT definition

CobiT defines control over defining and managing service levels in an IT environment:

> Control over the IT process **Define and Manage Service Levels**, with the business goal of establishing a common understanding of the level of service required, is enabled by the establishment of service-level agreements, which formalise the performance criteria against which the quantity and quality of service will be measured.[26]

According to CobiT, this control ensures delivery of information to the business that addresses the required information criteria (primarily, effectiveness and efficiency) and is measured by key goal indicators. The control considers critical success factors that leverage specific IT resources and is measured by key performance indicators.

Controls

*The following control objectives are based on CobiT guidelines for **Define and Manage Service Levels**. The control objectives were used by the ANAO in considering Health's management of IT service levels. The guidelines are provided here for consideration by Health for inclusion in the development of its service level policies and processes.*

Service level agreement framework

Management should define a framework wherein it promotes the definition of formal service level agreements and defines the minimal contents: availability, reliability, performance, capacity for growth, levels of support provided to users, continuity planning, security, minimum acceptable level of satisfactorily delivered system functionality, restrictions (limits on the amount of work), service charges, central print facilities (availability), central print distribution and change procedures. Users and the IT function should have a written agreement that describes the service level in qualitative and quantitative terms. The agreement defines the responsibilities of both parties. The IT function must offer the agreed quality and quantity of service and the users must constrain the demands they place upon the service within the agreed limits.

[26] Management Guidelines, CobiT, 3rd Ed., July 2000, IT Process DS1: *'Define and Manage Service Levels' (Delivery and Support),* p. 62.

Aspects of service level agreements

Explicit agreement should be reached on the aspects that a service level agreement should have. The service level agreement should cover at least the following aspects: availability, reliability, performance, capacity for growth, levels of support provided to users, continuity planning, security, minimum acceptable level of satisfactorily delivered system functionality, restrictions (limits on the amount of work), service charges, central print facilities (availability), central print distribution and change procedures.

Performance procedures

Procedures should be put in place to ensure that the manner of and responsibilities for performance governing relations (e.g. non-disclosure agreements) between all the involved parties are established, coordinated, maintained and communicated to all affected departments.

Monitoring and reporting

Management should appoint a service level manager who is responsible for monitoring and reporting on the achievement of the specified service performance criteria and all problems encountered during processing. The monitoring statistics should be analysed on a timely basis. Appropriate corrective action should be taken and failures should be investigated.

Review of service level agreements and contracts

Management should implement a regular review process for service level agreements and underpinning contracts with third-party service providers.

Chargeable items

Provisions for chargeable items should be included in the service level agreements to make trade-offs possible on service levels versus costs.

Service improvement program

Management should implement a process to ensure that users and service level managers regularly agree on a service improvement program for pursuing cost-justified improvements to the service level.

Measures

Critical Success Factors

CobiT outlines the critical success factors associated with define and manage service levels.

- Service levels are expressed in end-user business terms, wherever possible.
- Root cause analysis is performed when service levels breaches occur.
- Skills and tools are available to provide useful and timely service level information.
- The reliance of critical business processes on IT is defined and is covered by service level agreements.
- IT management accountabilities and responsibilities are linked to service levels.
- The IT organisation can identify sources of cost variances.
- Detailed and consistent explanations for cost variances are provided.
- A system for tracking and following individual changes is available.

Key Performance Indicators

CobiT outlines key performance indicators associated with define and manage service levels.

- Time lag of resolution of a service level change request.
- Frequency of customer satisfaction surveys.
- Time lag to resolve a service level issue.
- Number of times that root cause analysis of service level procedure and subsequent resolution is completed within required period.
- Significance of amount of additional funding needed to deliver the defined service level.

Key Goal Indicators

CobiT outlines key goal indicators associated with define and manage service levels.

- Sign-off by strategic business unit that service levels are aligned with key business objectives.
- Customer satisfaction that the services level meets expectations.
- Actual to budget cost ratio in line with service levels.

- Per cent of all critical business processes relying on IT covered by service level agreements.
- Per cent of service level agreements reviewed at the agreed interval or following major change.
- Service level partners sign-off service level monitoring information provided.
- Per cent of IT services, which met service level agreements.

Appendix 4

Ensure Systems Security: Definition, Controls and Measures

CobiT definition

CobiT defines control over ensuring systems security in an IT environment:

> Control over the IT process **Ensure Systems Security**, with the business goal of safeguarding information against unauthorised use, disclosure or modification, damage or loss, is enabled by logical access controls, which ensure that access to the systems, data and programs is restricted to authorised users.[27]

According to CobiT, this control ensures delivery of information to the business that addresses the required information criteria (primarily, confidentiality and integrity) and is measured by key goal indicators. The control considers critical success factors that leverage specific IT resources and is measured by key performance indicators.

Controls

*The following control objectives are based on CobiT guidelines for **Ensure Systems Security**. The control objectives were used by the ANAO in considering Health's IT security. The guidelines are provided here for consideration by Health for inclusion in the development of its security policies and practices.*

Manage security measures

IT security should be managed such that security measures are in line with business requirements. This includes:

- Translating risk assessment information to the IT security plans.
- Implementing the IT security plan.
- Updating the IT security plan to reflect changes in the IT configuration.
- Assessing the impact of change requests on IT security.
- Monitoring the implementation of the IT security plan.
- Aligning IT security procedures to other policies and procedures.

[27] Management Guidelines, CobiT, 3rd Ed., July 2000, IT Process DS5: *'Ensure Systems Security' (Delivery and Support),* p. 70.

Identification, authentication and access

The logical access to and use of IT computing resources should be restricted by the implementation of adequate identification, authentication and authorisation mechanisms, linking users and resources with access rules. Such mechanisms should prevent unauthorised personnel, dial-up connections and other system (network) entry ports from accessing computer resources and minimise the need for authorised users to use multiple sign-ons. Procedures should also be in place to keep authentication and access mechanisms effective (e.g. regular password changes).

Security of outline access to data

In an on-line IT environment, IT management should implement procedures in line with the security policy that provides access security control based on the individual's demonstrated need to view, add, change or delete data.

User account management

Management should establish procedures to ensure timely action relating to requesting, establishing, issuing, suspending and closing of user accounts. A formal approval procedure outlining the data or system owner granting the access privileges should be included. The security of third-party access should be defined contractually and address administration and non-disclosure requirements. Outsourcing arrangements should address the risks, security controls and procedures for information systems and networks in the contract between the parties.

Management review of user accounts

Management should have a control process in place to review and confirm access rights periodically. Periodic comparison of resources with recorded accountability should be made to help reduce the risk of errors, fraud, misuse or unauthorised alteration.

User control of user accounts

Users should systematically control the activity of their proper account(s). Also information mechanisms should be in place to allow them to oversee normal activity as well as to be alerted to unusual activity in a timely manner.

Security surveillance

IT security administration should ensure that security activity is logged and any indication of imminent security violation is reported immediately to all who may be concerned, internally and externally and is acted upon in a timely manner.

Data classification

Management should implement procedures to ensure that all data are classified in terms of sensitivity by a formal and explicit decision by the data owner according to the data classification scheme. Even data needing ‘no protection’ should require a formal decision to be so designated. Owners should determine disposition and sharing of data, as well as whether and when programs and files are to be maintained, archived or deleted. Evidence of owner approval and data disposition should be maintained. Policies should be defined to support reclassification of information, based on changing sensitivities. The classification scheme should include criteria for managing exchanges of information between organisations, addressing both security and compliance with relevant legislation.

Central identification and access rights management

Controls are in place to ensure that the identification and access rights of users as well as the identity of system and data ownership are established and managed in a unique and central manner to obtain consistency and efficiency of global access control.

Violation and security activity reports

IT security administration should ensure that violation and security activity is logged, reported, reviewed and appropriately escalated on a regular basis to identify and resolve incidents involving unauthorised activity. The logical access to the computer resources accountability information (security and other logs) should be granted based upon the principle of least privilege or need-to-know.

Incident handling

Management should establish a computer security incident handling capability to address security incidents by providing a centralised platform with sufficient expertise and equipped with rapid and secure communication facilities. Incident management responsibilities and procedures should be established to ensure an appropriate, effective and timely response to security incidents.

Re-accreditation

Management should ensure that re-accreditation of security (e.g. through ‘tiger teams’) is periodically performed to keep up-to-date the formally approved security level and the acceptance of residual risk.

Counter party trust

Organisational policy should ensure that control practices are implemented to verify the authenticity of the counter-party providing electronic instructions or transactions. This can be implemented through trusted exchange of passwords, tokens or cryptographic keys.

Transaction authorisation

Organisational policy should ensure that, where appropriate, controls are implemented to provide authenticity of transactions and establish the validity of a user’s claimed identity to the system. This requires use of cryptographic techniques for signing and verifying transactions.

Non-repudiation

Organisational policy should ensure that, where appropriate, transactions cannot be denied by either party and controls are implemented to provide non-repudiation of origin or receipt, proof of submission and receipt of transactions. This can be implemented through digital signatures, time stamping and trusted third-parties, with appropriate policies that take into account relevant regulatory requirements.

Trusted path

Organisational policy should ensure that sensitive transaction data is only exchanged over a trusted path. Sensitive information includes security management information, sensitive transaction data, passwords and cryptographic keys. To achieve this, trusted channels may need to be established using encryption between users, between users and systems and between systems.

Protection of security functions

All security related hardware and software should at all times be protected against tampering to maintain their integrity and against disclosure of secret keys. In addition organisations should keep a low profile about their security design, but should not base their security on the design being secret.

Cryptographic key management

Management should define and implement procedures and protocols to be used for generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorised disclosure. If a key is compromised, management should ensure this information is propagated to any interested party through the use of Certificate Revocation Lists or similar mechanisms.

Malicious software prevention, detection and correction

Regarding malicious software, such as computer viruses or Trojan horses, management should establish a framework of adequate preventative, detective and corrective control measures and occurrence response and reporting. Business and IT management should ensure that procedures are established across the organisation to protect information systems and technology from computer viruses. Procedures should incorporate virus protection, detection, occurrence response and reporting.

Firewall architectures and connections with public networks

If connection to the Internet or other public networks exists, adequate firewalls should be operative to protect against denial of services and any unauthorised access to the internal resources; should control any application and infrastructure management flows in both directions; and should protect against denial of service attacks.

Protection of electronic value

Management should protect the continued integrity of all cards or similar physical mechanisms used for authentication or storage of financial or other sensitive information, taking into consideration the related facilities, devices, employees and validation methods used.

Measures

Critical Success Factors

CobiT outlines the critical success factors associated with ensure system security.

- An overall security plan is developed that covers the building of awareness, establishes clear policies and standards, identifies a cost-effective and sustainable implementation and defines monitoring and enforcement processes.

- There is awareness that a good security plan takes time to evolve.
- The corporate security function reports to senior management and is responsible for executing the security plan.
- Management and staff have a common understanding of security requirements, vulnerabilities and threats and they understand and accept their own security responsibilities.
- Third-party evaluation of security policy and architecture is conducted periodically.
- A *'building permit'* program is defined, identifying security baselines that have to be adhered to.
- A *'drivers license'* program is in place for those developing, implementing and using systems, enforcing security certification of staff.
- The security function has the means and ability to detect, record, analyse significance, report and act upon security incidents when they do occur, while minimising the probability of occurrence by applying intrusion testing and active monitoring.
- A centralised user management process and system provides the means to identify and assign authorisations to users in a standard and efficient manner.
- A process is in place to authenticate users at reasonable cost, light to implement and easy to use.

Key Performance Indicators

CobiT outlines key performance indicators associated with ensure system security.

- Reduced number of security-related service calls, change requests and fixes.
- Amount of down-time, caused by security incidents.
- Reduced turn-around time for security administration requests.
- Number of systems subject to an intrusion detection process.
- Number of systems with active monitoring capabilities.
- Reduced time to investigate security incidents.
- Time-lag between detection, reporting and acting upon security incidents.
- Number of IT security awareness training days.

Key Goal Indicators

CobiT outlines key goal indicators associated with ensure system security.

- No incidents causing public embarrassment.
- Immediate reporting on critical incidents.
- Alignment of access rights with organisational responsibilities.
- Reduced number of new implementations delayed by security concerns.
- Full compliance or agreed and recorded deviations from minimum security requirements.
- Reduced number of incidents involving unauthorised access, loss or corruption of information.

Appendix 5

Monitor the Processes: Definition, Controls and Measures

CobiT definition

CobiT defines control over monitoring the processes in an IT environment:

> Control over the IT process **Monitor the Processes**, with the business goal of ensuring the achievement of the performance objectives set for the IT processes, is enabled by the definition of relevant performance indicators, the systematic and timely reporting of performance and prompt acting upon deviations.[28]

According to CobiT, this control ensures the delivery of information to the business that addresses the required information criteria (primarily, effectiveness and efficiency) and is measured by key goal indicators. The control considers critical success factors that leverage specific IT resources and is measured by key performance indicators.

Controls

*The following control objectives are based on CobiT guidelines for **Monitor the Processes**. The control objectives were used by the ANAO in considering Health's monitoring of IT. The guidelines are provided here for consideration by Health for inclusion in the development of its monitoring policies, plans and processes.*

Collecting monitoring data

For the IT and internal control processes, management should ensure relevant performance indicators (e.g. benchmarks) from both internal and external sources are being defined and that data is being collected for the creation of management information reports and exception reports regarding these indicators. Controls should also be aimed at validating the propriety and integrity of both organisational and individual performance measures and indicators.

Assessing performance

Services to be delivered by the IT function should be measured (key performance indicators and/or critical success factors) by management and be compared with target levels. Assessments of the IT function should be performed on a continuous basis.

[28] Management Guidelines, CobiT, 3rd Ed., July 2000, IT Process M1: *'Monitor the Processes' (Monitoring),* p. 90.

Assessing customer satisfaction

At regular intervals management should measure customer satisfaction regarding the services delivered by the IT function to identify shortfalls in service levels and establish improvement objectives.

Management reporting

Management reports should be provided for senior management's review of the organisation's progress toward identified goals. Status reports should include the extent to which planned objectives have been achieved, deliverables obtained, performance targets met and risks mitigated. Upon review, appropriate management action should be initiated and controlled.

Measures

Critical Success Factors

CobiT outlines the critical success factors associated with monitor the processes.

- Useful, accurate and timely management reports are available.
- Processes have defined and understood Key Goal Indicators and Key Performance Indicators.
- Measurements of IT performance include financial, operational, customer and organisational learning criteria that ensure alignment with organisation-wide goals and can be integrated with tools such as the IT Balanced Business Scorecard.
- There are clearly understood and communicated process objectives.
- A framework is established for defining and implementing IT governance reporting requirements.
- A knowledge base of historical performance is established.

Key Performance Indicators

CobiT outlines key performance indicators associated with monitor the processes.

- Time-lag between the process deficiency occurrence and reporting.
- Time-lag between the reporting of a deficiency and action initiated.
- Ratio between process deficiencies reported and deficiencies subsequently accepted as requiring management attention follow-up ('noise index').
- Number of processes monitored.

- Number of cause and effect relations identified and incorporated in monitoring.
- Number of external benchmarks of process effectiveness.
- Time-lag between business change and associated performance indicators.
- Number of changes to performance indicators without the business goals changing.

Key Goal Indicators

CobiT outlines key goal indicators associated with monitor the processes.

- Consistent application of the right limited number of performance indicators.
- Increased number of process improvement opportunities detected and acted upon.
- Satisfaction of management and the governance entity with performance reporting.
- Reduced number of outstanding process deficiencies.

Appendix 6

IT Governance: Definition and Measures

CobiT definition

The ANAO used the CobiT definition of IT governance which states:

> Governance over information technology and its processes, with the business goal of adding value, while balancing risk versus return, is enabled by creating and maintaining a system of process and control excellence appropriate for the business that directs and monitors the business value delivery of IT.[29]

According to CobiT, governance over IT and its processes ensures delivery of information to the business that addresses the required information criteria and is measured by key goal indicators. Governance over IT and its processes considers critical success factors that leverage all IT resources and is measured by key performance indicators.

Measures

Critical success factors

CobiT outlines the critical success factors associated with IT Governance.

- IT governance activities are integrated into the enterprise governance process and leadership behaviours.
- IT governance focuses on the enterprise goals, strategic initiatives, the use of technology to enhance the business and on the availability of sufficient resources and capabilities to keep up with the business demands.
- IT governance activities are defined with a clear purpose, documented and implemented, based on enterprise needs and with unambiguous accountabilities.
- Management practices are implemented to increase efficient and optimal use of resources and increase the effectiveness of IT processes.
- Organisational practices are established to enable: sound oversight; a control environment / culture; risk assessment as standard practice; degree of adherence to established standards; monitoring and follow up of control deficiencies and risks.

[29] Management Guidelines, CobiT, 3rd Ed., July 2000, Appendix V: *'IT Governance Management Guideline',* p. 120.

- Control practices are defined to avoid breakdowns in internal control and oversight.
- There is integration and smooth interoperability of the more complex IT processes such as problem, change and configuration management.
- An audit committee is established to appoint and oversee an independent auditor, focusing on IT when driving audit plans and reviews the results of audits and third-party reviews.

Key performance indicators

CobiT outlines key performance indicators associated with managing quality.

- Improved cost-efficiency of IT processes (cost vs. deliverables).
- Increased number of IT action plans for process improvement initiatives.
- Increased utilisation of IT infrastructure.
- Increased satisfaction of stakeholders (survey and number of complaints).
- Improved staff productivity (number of deliverables) and morale (survey).
- Increased availability of knowledge and information for managing the enterprise.
- Increased linkage between IT and enterprise governance.
- Improved performance, as measured by IT balanced scorecards.

Key goal indicators

CobiT outlines key goal indicators associated with managing quality.

- Enhanced performance and cost management.
- Improved return on major IT investments.
- Improved time to market.
- Increased quality, innovation and risk management.
- Appropriately integrated and standardised business processes.
- Reaching new and satisfying existing customers.
- Availability of appropriate bandwidth, computing power and IT delivery mechanisms.
- Meeting requirements and expectations of the customer of the process on budget and on time.

- Adherence to laws, regulations, industry standards and contractual commitments.
- Transparency on risk-taking and adherence to the agreed organisational risk profile.
- Benchmarking comparisons of IT governance maturity.
- Creation of new service delivery channels.

Index

Better Practice Guides

Administration of Grants	May 2002
Performance Information in Portfolio Budget Statements	May 2002
Life-Cycle Costing	Dec 2001
Some Better Practice Principles for Developing Policy Advice	Nov 2001
Rehabilitation: Managing Return to Work	Jun 2001
Internet Delivery Decisions	Apr 2001
Planning for the Workforce of the Future	Mar 2001
Contract Management	Feb 2001
AMODEL Illustrative Financial Statements 2001	May 2001
Business Continuity Management	Jan 2000
Building a Better Financial Management Framework	Nov 1999
Building Better Financial Management Support	Nov 1999
Managing APS Staff Reductions (in Audit Report No.49 1998–99)	Jun 1999
Commonwealth Agency Energy Management	Jun 1999
Corporate Governance in Commonwealth Authorities and Companies–Principles and Better Practices	Jun 1999
Managing Parliamentary Workflow	Jun 1999
Cash Management	Mar 1999
Management of Occupational Stress in Commonwealth Agencies	Dec 1998
Security and Control for SAP R/3	Oct 1998
Selecting Suppliers: Managing the Risk	Oct 1998
New Directions in Internal Audit	Jul 1998
Controlling Performance and Outcomes	Dec 1997
Management of Accounts Receivable	Dec 1997
Protective Security Principles (in Audit Report No.21 1997–98)	Dec 1997
Public Sector Travel	Dec 1997

Audit Committees	Jul 1997
Core Public Sector Corporate Governance (includes Applying Principles and Practice of Corporate Governance in Budget Funded Agencies)	Jun 1997
Administration of Grants	May 1997
Management of Corporate Sponsorship	Apr 1997
Telephone Call Centres	Dec 1996
Telephone Call Centres Handbook	Dec 1996
Paying Accounts	Nov 1996
Performance Information Principles	Nov 1996
Asset Management	Jun 1996
Asset Management Handbook	Jun 1996
Managing APS Staff Reductions	Jun 1996