The Auditor-General
Audit Report No.44 2000–2001
Performance Audit

Information Technology in the Department of Veterans' Affairs

Department of Veterans' Affairs

Australian National Audit Office

ISSN 1036-7632

ISBN 0 642 44222 3

Australian National
Audit Office

Canberra ACT
5 June 2001

Dear Madam President
Dear Mr Speaker

The Australian National Audit Office has undertaken a performance audit in the Department of Veterans' Affairs 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 in the Department of Veterans' Affairs.*

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

Yours sincerely

P. J. Barrett
Auditor-General

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

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

Eric Turner

Paul Nicoll

Contents

Abbreviations/Glossary

ACF2	Security software that manages individual's access to programs and data on large computers
ANAO	Australian National Audit Office
BCP	Business Continuity Plan
CCPS	Compensation Claims Processing System
CobiT	Control Objectives for Information and Related Technology
DVA	Department of Veterans' Affairs
EMG	Executive Management Group
FMIS	Financial Management Information System
IBM GSA	International Business Machines Global Services Australia
IBMA	International Business Machines Australia
IMU	Information Management Unit
IT	Information Technology
NAFCOM	National Audit and Fraud Committee
PIPS	Pension Information Processing System
QA	Quality Assurance
SPRB	Strategic Planning Review Board
VIEW	Veteran Information Enquiry Window
Windows NT	A Microsoft operating system for computers and servers

Summary and Recommendations

Summary

1. The Department of Veterans' Affairs (DVA) is responsible for major programs assisting war veterans and their dependents. The services include:

- compensation and income support pensions and a range of associated benefits and allowances; and
- provision of medical treatment, counselling services and other related services.

2. In 1999–2000, the department paid in excess of 380 000 income support pensions, and approximately 270 000 compensation pensions, as well as providing health services to some 349 000 veterans. The department received over 54 500 claims for new or increased compensation payments. The department estimates the total veteran population of Australia at 480 000. In 2000–2001, income support payments by DVA are expected to be $5.4 billion out of a total departmental budget of around $8.5 billion. DVA has the fourth largest appropriation to administer amongst Commonwealth agencies.

3. DVA outsourced its information technology (IT) infrastructure in February 1992, becoming the first Commonwealth agency to outsource a major part, or all, of its IT operations. At the time of the audit, DVA's IT operations had been outsourced for about eight years. The present contractor is IBM Australia (IBMA), together with IBM GSA. A separate ANAO audit is examining the management of the IT outsourcing contract by the department.

4. This audit reviewed IT systems used to support the department's income support and compensation responsibilities. Most attention was given to those systems entitled the Veteran Information Enquiry Window (VIEW), the Pension Information Processing System (PIPS), and the Compensation Claims Processing System (CCPS). Information about each of these systems is included in Appendix 1. From a financial statement perspective, two other systems were also reviewed. These were a financial management information system known as DOLARS, and a human resource management system called PAHRIS. The conclusions drawn in this report are based largely on an examination of VIEW, PIPS and CCPS. However, the conclusions are also likely to be applicable to the department's IT systems as a whole.

Audit objective and approach

5. The audit was conducted as a joint financial statement and performance audit of DVA's IT systems. The objective of the financial statement component of the audit was to express an opinion on whether DVA could rely on its IT systems to support production of a reliable set of balances for the financial statements. The objective of the performance audit component was to determine whether DVA's IT systems' outputs met quality and service delivery targets.

6. Building on the work undertaken during the financial statement audit, the ANAO conducted additional analyses of some other aspects of DVA's IT systems. This report provides the ANAO's findings and conclusions as a result of the additional analyses. The additional analysis aimed to:

- identify sound practice and any deficiencies in IT controls and any resulting effect on the department's operations;
- determine whether the IT systems outputs meet quality and service delivery parameters set by the department; and
- identify aspects of system management that can be applied more generally by the department.

7. The first phase of the audit addressed the financial statement aspects which results are reprinted in Chapter 2. The second phase of the audit encompassed the performance aspects of the audit objective. The audit team considered that these latter aspects were best addressed using an international set of standards, particularly given the global nature of information technology. The Information Systems Audit and Control Foundation has developed standards, known as CobiT (Control Objectives for Information and Related Technology). CobiT standards are tools generally applicable to, and are an accepted standard for, IT governance. Appendix 2 provides further information about the CobiT standards. The IT systems of the department were measured against the CobiT standards and the criteria embedded in those standards.

8. The CobiT process and control objectives fall into four main domains:

- planning and organisation of IT (addressed in Chapter 3 of this report);
- developing and maintaining IT procedures (Chapter 4);
- IT delivery and support (Chapter 5); and
- monitoring (Chapter 6).

9. Due to issues of relevance, time and cost constraints, the audit did not address all the specific control objectives within these four main domains. The audit did, however, concentrate on controls important to DVA's business.

Overall audit conclusion

10. The ANAO concluded that, overall, DVA's management of its IT systems was satisfactory. In regard to specific audit objectives, the ANAO concluded that:

- the results of testing indicated that reliance could be placed on DVA's IT systems and controls, and accuracy of the accounts and records, to the extent necessary to form an opinion on the department's financial statements; and
- the outputs of the three systems used to support DVA's income support and compensation responsibilities met DVA's quality and service delivery performance parameters.

11. The ANAO's additional analyses, referred to in paragraph 6 above, also concluded that:

- DVA's planning and organisation of IT was satisfactory. DVA, on the basis of sound practice against the CobiT objectives for planning and organisation, has formal accreditation of its IT quality management procedures against internationally recognised standards for quality management. In addition, DVA uses an industry-recognised system development life cycle methodology for development and maintenance of its IT systems;
- DVA's IT delivery and support controls require some improvement over the local area network and windows environment, and particularly in the regular review of access logs to IT systems; and
- DVA had only a limited ability to identify the costs of the use of IT to deliver services, and to link IT system performance measures directly to client quality and performance targets.

12. A summary of the ANAO conclusions against each of the CobiT domains, and against each CobiT objective within the domains, is given in Table 1 in Chapter 1.

Key Findings

Planning and organisation (Chapter 3): this component of the audit aimed to identify the link between DVA's business objectives and its IT strategies.

13. DVA had in place sound planning and organisation systems. However, the ANAO found there was a lack of a clear linkage between internal IT system performance measures and agreed client quality and performance targets reported in the Balanced Scorecard for Income Support and Compensation. This could limit the effectiveness of the department's IT planning to support its business objectives. Clearly documented mechanisms for reporting actual performance of IT operations against IT measures would also assist DVA to meet the objectives of its IT Strategic Plan.

14. The ANAO also found that DVA's documentation of its information architecture was substantially incomplete, although the department was undertaking this task during the audit. Given the dynamic nature of DVA's Income Support and Compensation related systems, changes and revisions to all relevant documentation should occur promptly for both management and business continuity purposes.

Developing and maintaining IT procedures and managing change (Chapter 4): *this component of the audit aimed to determine whether DVA effectively developed and maintained its IT procedures, and adequately controlled changes to its IT systems.*

15. DVA's change management process was considered to be satisfactory. However, issues were identified relating to the timeliness of change requests, where several change requests for CCPS classified as major had not been actioned for over six months. If major changes are not being actioned on a timely basis, there could be an adverse impact on quality and timeliness of processing resulting in sub-standard performance.

16. The ANAO found that user, operational and technical procedures had been documented and adequately maintained. These procedures were also found to address adequately existing service levels and operational requirements.

Delivery and support (Chapter 5): *this component of the audit aimed to identify the support process and controls put in place by DVA to ensure the actual delivery of the required IT services.*

17. DVA had identified its IT performance requirements; ensured continuous service from the three systems reviewed; had adequate systems security control arrangements; had undertaken work to identify the costs of its IT operations; and had managed problems and incidents satisfactorily.

Monitoring (Chapter 6): *this component of the audit aimed to determine whether monitoring arrangements allowed HIC's managers to assess the quality of IT processes and compliance with control requirements.*

18. DVA's internal system performance measures were found to be generally satisfactory. DVA adequately monitored its system performance, and the department had adequate independent assurance for its systems. However, acceptable performance variations from IT system targets had not been developed for performance management purposes.

Recommendations

Each of the following recommendations will assist in development of DVA's systems.

Recommendation No.1 Para. 4.9

The ANAO recommends that DVA monitor the time taken to implement changes of its application software, from initiation of a change to its execution, to help ensure all changes which have a significant impact on the business are completed in a timely manner.

DVA response: Agreed.

Recommendation No.2 Para. 6.12

The ANAO recommends that DVA:

- formulate IT Balanced Scorecard measures that directly link, and relate to, relevant IT strategy statements. These measures would then enable effective monitoring of progress in implementing the IT strategic plan;
- develop suitable measures for IT systems that support DVA's client service reporting requirements;
- review and update the information systems model documentation to ensure it is complete and current to facilitate operations and any changes that may be required;
- clearly articulate in its balance scorecard reports:
  - inherent limitations on the accuracy of performance reports; and
  - clear explanations and definitions of key terms used in the reports, including what is meant by 'error' and 'accuracy'; and
- formalise acceptable variations from agreed targets for all internal and external IT system reporting.

DVA's Response: Agreed.

Audit Findings and Conclusions

1. Introduction

This chapter provides an overview of the Department of Veterans' Affairs and identifies the aspects of the department's information technology examined in the audit. The chapter also describes the audit objectives and methodology, and the structure of this report.

Background

1.1 The ANAO contracted Deloitte Touche Tohmatsu to assist with the audit of information technology (IT) in three Commonwealth agencies, Centrelink, the Health Insurance Commission and the Department of Veterans' Affairs.

1.2 The result of the audit of each agency is reported separately. This report covers the audit of the Department of Veterans' Affairs.

The Department of Veterans' Affairs

1.3 The Department of Veterans' Affairs is responsible for major programs assisting war veterans and their dependents. DVA's services include:

- compensation and income support pensions and a range of associated benefits and allowances; and
- provision of medical treatment, counselling services and other related services.

1.4 DVA estimates the total veteran population of Australia at 480 000. In 1999–2000, DVA paid in excess of 380 000 income support pensions as well as providing health services to some 349 000 veterans. Also in that year, DVA received over 54 500 claims for new or increased compensation payments, and it paid approximately 270 000 compensation pensions. Compensation payments by DVA in 1999–2000 totalled some $4.75 billion out of a total departmental budget of around $7.76 billion. DVA has the fourth largest appropriation to administer amongst Commonwealth agencies.

1.5 DVA outsourced its IT in February 1992, becoming the first Commonwealth agency to outsource a major part, or all, of its IT operations. At the time of this audit, DVA's IT operations had been outsourced for approximately eight years. The present contractor is IBM Australia together with IBM GSA.

1.6 This audit reviewed IT systems used to support the DVA's income support and compensation responsibilities. The systems are the Veteran Information Enquiry Window (VIEW), the Pension Information Processing System (PIPS), and the Compensation Claims Processing System (CCPS). Information about each of these systems is included in Appendix 1. In summary, the systems are used for:

- client registration;
- validation of clients' eligibility;
- entitlement assessment;
- payment calculation;
- revision of payment detail; and
- generation of notifications and assessment letters.

1.7 From a financial statement perspective, two other systems were reviewed. These were a financial management information system called DOLARS, and a human resource management system called PAHRIS. The conclusions drawn in this report are based largely on an examination of VIEW, PIPS and CCPS. However, the conclusions are also likely to be applicable to the department's IT systems as a whole.

Audit objective

1.8 The audit was conducted as a joint financial statement and performance audit of DVA's IT systems. The objective of the financial statement component of the audit was to express an opinion on whether DVA could rely on its IT systems to support production of a reliable set of balances for the financial statements. The objective of the performance audit component was to determine whether DVA's IT systems' outputs met quality and service delivery targets.

1.9 Building on the work undertaken during the financial statement audit, the ANAO conducted additional analyses of some other aspects of DVA's IT systems. This report provides the ANAO's findings and conclusions as a result of the additional analyses. The additional analyses aimed to:

- identify sound practice and any deficiencies in IT controls and any resulting effect on the department's operations;
- determine whether the IT systems outputs meet quality and service delivery parameters set by the department; and
- identify aspects of system management that can be applied more generally by the department.

Audit approach, methodology and scope

1.10 The audit was conducted partly as an element of the annual examination of the financial statements of DVA, and partly as a performance audit of DVA's use of IT. The financial statement audit examined IT system controls with a view to forming an opinion on DVA's financial statements. An unqualified audit opinion on DVA's 1999–2000 financial statements was included in DVA's 1999–2000 Annual Report.[1]

1.11 The audit objectives were addressed by assessing key aspects of the three systems against selected, relevant control objectives of an international set of standards, particularly given the global nature of information technology. The Information Systems Audit and Control Association (ISACA) Foundation developed those standards. ISACA is a worldwide organisation based in the USA. The standards are called Control Objectives for Information and Related Technology, or CobiT[2]. CobiT standards are tools generally applicable to, and are an accepted standard for, good IT governance. The CobiT standards formed the audit criteria for the second part of the audit. They are summarised in Table 1. The Table includes the full set of CobiT objectives, whether addressed by the ANAO or not, and has been extended from the standard CobiT table to include:

- a summary of whether the ANAO considered that DVA had addressed that CobiT objective satisfactorily;
- an indication as to whether the ANAO had addressed a specific CobiT objective and where it had not due to issues of relevance, time and cost constraints; and
- a cross-reference to the paragraph in the report that addresses the CobiT objective.

1.12 The audit included a review of DVA's documentation and reports, and interviews with DVA staff. In addition a review was conducted of working papers provided by PriceWaterhouseCoopers on its analysis of the effectiveness of the control procedures of DVA's IT service provider, IBM GSA.

---

1 Department of Veterans' Affairs, 1999–2000 Annual Report DVA, Canberra, 2000. pp. 269–270.

2 CobiT copyright notice: *'Copyright 1996, 1998, 2000 Information Systems Audit and Control Foundation. Reprinted with the permission of the Information Systems Audit and Control Foundation and IT Governance Institute'*.

Report structure

1.13 Chapter 2 provides an overall summary of the results of the ANAO's financial statement audit component of this integrated audit.

1.14 The CobiT process and control objectives fall into four main domains. The findings about each of the four CobiT domains are reported in the following chapters:

- planning and organisation of IT (addressed in Chapter 3 of this report);
- developing and maintaining IT procedures (Chapter 4);
- IT delivery and support (Chapter 5); and
- monitoring (Chapter 6).

1.15 The audit was conducted in compliance with ANAO Auditing Standards. Its estimated cost was $337 444.

Table 1

Control Objectives for Information and Related Technology Process and Control Objectives—Summary Results for DVA

CobiT Process and Control Objectives		*Information criteria*[1]							*Rating*[2] *Scope*		
		Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	S'factory/Recomm	Not in scope[3]	Report Reference
	Planning and organisation										
P01	Define a strategic IT plan	P	S						✓		3.2
P02	Define the information architecture	P	S	S	S				✓		3.17
P03	Determine the technological direction	P	S							N	
P04	Define the IT organisation and relationships	P	S							N	
P05	Manage the IT investment	P	P					S	✓		3.21
P06	Communicate management aims and direction	P					S		✓		3.23
P07	Manage human resources	P	P							N	
P08	Ensure compliance with external requirements	P					P	S		N	
P09	Assess risks	S	P	P	P	S	S	S	✓		3.27
P10	Manage projects	P	P							N	
P11	Manage quality	P	P		P			S	✓		3.31
	Planning and organisation overall								✓		

CobiT Process and Control Objectives		*Information criteria*[1]							*Rating*[2] *Scope*		
		Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	S'factory/Recomm	Not in scope[3]	Report Reference
	Acquisition and implementation										
AI1	Identify solutions	P	S							N	
AI2	Acquire and maintain application software	P	P		S		S	S		N	
AI3	Acquire and maintain technology architecture	P	P		S					N	
AI4	Develop and maintain IT procedures	P	P		S		S	S	✓		4.2
AI5	Install and accredit systems	P			S	S				N	
AI6	Manage changes	P	P		P	P		S	R		4.5
	Acquisition and implementation overall								✓		
	Delivery and support										
DS1	Define service levels	P	P	S	S	S	S	S		N	
DS2	Manage third party service	P	P	S	S	S	S	S		N	
DS3	Manage performance and capacity	P	P			S			✓		5.3
DS4	Ensure continuous service	P	S			P			✓		5.8
DS5	Ensure systems security			P	P	S	S	S	✓		5.12
DS6	Identify and attribute costs		P					P	✓		5.20
DS7	Educate and train users	P	S							N	
DS8	Assist and advise IT customers	P								N	
DS9	Manage the configuration	P				S		S		N	
DS10	Manage problems and incidents	P	P			S			✓		5.22
DS11	Manage data				P			P		N	
DS12	Manage facilities				P	P				N	
DS13	Manage operations	P	P		S	S				N	
	Delivery and support overall								✓		
	Monitoring										
M1	Monitor the process	P	S	S	S	S	S	S	R		6.2
M2	Assess internal control adequacy	P	P	S	S	S	S	S	✓		6.22
M3	Obtain independent assurance	P	P	S	S	S	S	S	✓		6.24
M4	Provide for independent audit	P	P	S	S	S	S	S	✓		6.26
	Monitoring overall								✓		

Notes to table:

1 P = a primary criteria addressed by the objective, S = secondary, a blank cell indicates the objective does not address the information criteria.

2 R indicates an ANAO recommendation.

3 Within time and cost constraints, the ANAO concentrated on controls critical to DVA's business.

2. Financial Statement Audit

The ANAO reported the results of its audit relating to DVA's financial statements in Report No.52 of 1999–2000, Control Structures as Part of the Audits of Financial Statements of Major Commonwealth Agencies for the Period Ending June 2000.[3] *The relevant sections of the report are detailed below.*

Operating Environment

2.1 DVA has a number of operational systems used to process payments that range from payments of benefits to veterans to processing salaries for DVA employees.

2.2 In 1997, DVA's IT hardware and infrastructure were outsourced to IBM Australia and IBM GSA. DVA introduced its new financial management information system (FMIS) and human resource system (PAHRIS) during the 1998–99 financial year. The results of the 1999–2000 financial statement audit indicated that departmental systems and procedures are able to produce accurate and complete information for financial reporting purposes. However, improvements are still required in a number of areas before systems will be able to achieve their full potential.

Audit findings

2.3 The ANAO's examination identified matters requiring specific attention relating to the operational system controls, quality assurance processes, and reconciliations of the general ledger to the cash ledger and bank accounts. A number of the issues, discussed below, also were raised with the DVA as a result of the 1998–99 financial statement audit and departmental remedial action is still outstanding. Only matters relevant to IT are reported here.

DOLARS—Financial management information system

2.4 DVA has put in place a quality assurance framework over the processing of payments. Strong management commitment to the conduct and follow up of quality assurance processes is a necessary prerequisite to the effective operation of this key control. The quality assurance process is comprised of a review of a selected number of transactions on a periodic basis to ensure accuracy of data processing and compliance with departmental control instructions.

---

[3] ANAO, Report No.52 of 1999–2000, *Control Structures As Part of the Audits of Financial Statements of Major Commonwealth Agencies for the Period Ending June 2000*, ANAO, Canberra, 2000.

2.5 ANAO's review of the quality assurance process revealed significant backlogs, delays in analysis of related reports, and a high rate of errors. As part of the audit whose results are reported here, the ANAO recommended that, in regard to business and operational risks, departmental management should assess the priority and adequacy of resources devoted to critical quality assurance processes. ANAO proposed during the audit that this assessment should focus on ensuring the timeliness of monitoring so that remedial action can be undertaken in a timely manner. DVA has now taken this action.

Benefit processing

2.6 Apart from its quality assurance processes over departmental expenses, DVA has also implemented quality assurance processes over benefit payments. The timeliness of these processes, and effective management analysis and immediate preventive action resulting from such processes are significant management controls over the accuracy of data processed through the department's computerised accounting systems. It is acknowledged that the Income Support quality assurance program is being redesigned to bring uniformity across all States. However, there were delays in the department's consolidation of income support pension quality assurance reports, inconsistencies in their evaluation, and a lack of quantification and action taken on critical errors. In this case, critical errors refer to problems in the application of financial controls. The department has now addressed these issues.

2.7 DVA advised that a new quality assurance (QA) program was developed and implemented from 1 July 2000. This is a comprehensive QA program which involves a 5 per cent sampling regime with a bias towards higher risk cases. The QA program has well-defined case assessment criteria and detailed error definitions. The program is supported by an IT system that provides for the sample selection, on-line recording of case assessments by QA officers, and a wide range reporting capability. These include reports on cases of critical errors, numbers of high and low impact errors, and the nature and incidence of errors by high to low level assessment criteria. A key objective of the new reporting capability is to enable the identification of best practice, training needs, and to provide feedback to individual decision-makers in a timely manner. The aim is to improve the performance of individual decision-makers, continually monitoring their performance and taking action towards continuous improvement. Comprehensive quarterly QA reports are being prepared and distributed in a timely manner. In addition, improved error definitions are providing a more accurate assessment of performance than previously occurred, and training programs and performance feedback measures are in place.

2.8 During the audit, the following system deficiencies were noted in a State Office:

- reports were not produced to identify clients with duplicate registrations on the Pension Payments Systems. The department has since advised that a new client registration system has been introduced which introduced a unique identifying number for every client. This virtually eliminated the possibility of duplicate registration of clients. DVA acknowledged that it was possible for many registrations to take place for the same client in PIPS and CCPS, but that it was valid for this to occur. Due to system controls, only one of these registrations could be processed to payment; and
- inadequate processing controls, such as providing confirmations that the IT environment was operating as approved. DVA advised that new certification procedures had been introduced, and that these were based on formal risk assessments conducted jointly with internal audit. Regular certifications of system compliance were required from appropriate DVA personnel. Certification specifically addressed whether the IT environment operated correctly and reported on any problems.

PAHRIS—Human resource system

2.9 For the financial statement audit, the department's human resource system, (PAHRIS) was also reviewed. PAHRIS produces the financially material employee entitlement balances. The ANAO found there is no review of the data entry to the program for leave entitlement calculations and no regular management review of reports to detect any inaccuracy. In addition, there is no application control within PAHRIS to prevent any exceptions or data entry error. In light of the reduced financial reporting timetable, the ANAO considers it even more appropriate for DVA to maintain accurate and timely accrual accounting systems. As a consequence, the ANAO recommended that management implements operational controls and review processes to ensure accurate data on leave entitlements.

IT systems and controls

2.10 The ANAO also found that controls in the local area network, windows environment, and particularly in respect to the regular review of access logs require improvement.

2.11 DVA is documenting its policies and procedures to monitor access to the local area network and windows environment. This monitoring will provide an assurance that users of the local area network and windows environment are accountable for their actions.

2.12 DVA acknowledged the issues raised and is giving priority to establishing policies and procedures to minimise the risk of irregularities occurring and to enhancing its control framework.

Conclusion

2.13 The ANAO financial statement information technology (IT) audit found that the results of testing indicated that reliance could be placed on DVA IT systems and controls, and accuracy of the accounts and records, to the extent necessary to form an opinion on the department's financial statements.

3. IT Planning and Organisation

This chapter reviews key aspects of DVA's IT planning and organisation. In particular, it comments on IT strategic planning, organisation of information systems, management of the IT investment, management's communication of its aims and directions, risk assessment and quality management.

3.1 The CobiT domain *IT planning and organisation* addresses the audit objectives of identifying sound practice, and determining whether the IT systems meet quality and service delivery parameters set by the department. It is sound practice to develop IT plans that identify the way IT can best contribute to the achievement of business objectives. These strategies need to be planned, communicated and managed. Table 2 below summarises the CobiT objectives for this domain and the conclusions reached against those objectives by the ANAO.

Table 2

Control Objectives for Information and Related Technology Process and Control Objectives—Planning and Organisation

CobiT Process and Control Objectives		*Information criteria*[1]							*Rating*[2] *Scope*		
		Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	S'factory/Recomm	Not in scope[3]	Report Reference
	Planning and organisation										
P01	Define a strategic IT plan	P	S						✓		3.2
P02	Define the information architecture	P	S	S	S				✓		3.17
P03	Determine the technological direction	P	S							N	
P04	Define the IT organisation and relationships	P	S							N	
P05	Manage the IT investment	P	P					S	✓		3.21
P06	Communicate management aims and direction	P					S		✓		3.23
P07	Manage human resources	P	P							N	
P08	Ensure compliance with external requirements	P					P	S		N	
P09	Assess risks	S	S	P	P	P	S	S	✓		3.27
P10	Manage projects	P	P							N	
P11	Manage quality	P	P		P			S	✓		3.31
	Planning and organisation overall								✓		

Notes to table:

1 P = a primary criteria addressed by the objective, S = secondary, a blank cell indicates the objective does not address the information criteria.

2 R indicates an ANAO recommendation.

3 Within time and cost constraints, the ANAO concentrated on controls critical to DVA's business

Strategic IT planning

3.2 The ANAO sought to establish whether the department had:

- a structured approach to IT planning;
- a methodology to formulate and modify IT plans;
- considered its vision and purpose in its IT strategic planning; and
- conducted risk assessments of IT initiatives.

3.3 The ANAO examined two dimensions of the department's IT strategic planning. The first dimension was organisational in that it identified whether DVA's vision and purpose played a part in the department's IT strategic planning. The second dimension was in regard to information technology, including initiatives such as the VIEW common platform and the PIPS and CCPS applications and surrounding business process. The common platform permits DVA staff to have easier access to DVA's software for delivery of its services. In its examination of these two dimensions, the ANAO reviewed the consistency and congruence of the following departmental documentation:

- organisation and IT Balanced Scorecards;
- IT strategic plan management and monitoring structures; and
- IT strategic plans.

Organisational planning

3.4 DVA has a planning framework that includes a Service Charter, Corporate Plan and a Strategic Planning and Reporting Framework.

3.5 Organisation planning culminates in, and is communicated by, a mission statement, a vision statement and a list of core behaviours and values for DVA. Planning for VIEW, PIPS and CCPS applications and associated business processes exists within this context.

3.6 DVA has five performance outcomes from the planning process which relate to:

- veterans' compensation;
- military compensation;
- care of veterans;
- commemoration of significant military events; and
- client service.

3.7 The department records its performance from the planning process in the National Balanced Scorecard and in local Balanced Scorecards. Local Balanced Scorecards are designed to align to the National Balanced Scorecard to monitor performance at various levels. An IT Balanced Scorecard has also been developed to measure IT operational activities.

Strategic IT planning

3.8 Leadership in IT and accountability for DVA IT services and outputs resides with the DVA Information Management Unit (IMU). The IMU was established to determine and realise the frameworks, principles and processes for IT at DVA. It reports to the Executive Management Group. An Information Management Steering Committee (IMSC) is established within the IMU to determine, implement and manage the IT strategic and business plans having regard to the department's business strategy, business priorities, and technology capability, amongst other considerations. IMSC's membership includes the Information Manager, the Business and Infrastructure Services Manager, the Corporate Applications Manager, and the Veterans' Services Applications Manager.

3.9 The IMU uses a rolling five year IT Strategic Planning cycle that starts in July-August of each year. At the time of the audit, DVA was revising the IT Strategic Plan for 2000–2005. This revision resulted in the identification of organisation-wide IT strategies and related plans. During the audit, the IMU's Strategic Planning Review Board (SPRB) was considering the results of this process.

3.10 The key outcomes of the IT Strategic Planning process were the identification of specific IT strategies linked to business objectives. There were no IT Balanced Scorecard measures for each IT strategy statement to enable departmental monitoring of its implementation of the IT Strategic Plan. In other words, the department had not developed IT Balanced Scorecard measures to systematically align business and IT goals and measures.

3.11 The department requires a framework for the use of IT system performance standards, targets, benchmarks and comparisons over time if its performance information is to be useful both for performance improvement and accountability.

VIEW, CCPS & PIPS IT systems planning

3.12 DVA has many performance indicators for levels of service to be provided to clients. These include performance indicators such as timeliness, accuracy and quantity of claims processed, and timeliness and accuracy of decisions. These measures form the basis of the Balanced Scorecard reported quarterly to the Executive Management Group (EMG).

3.13 It was noted that most of the client performance indicators relate to Income Support and Compensation Divisions of DVA. VIEW, CCPS and PIPS are the primary systems that assist Income Support and Compensation.

3.14 The ANAO found that DVA had developed some specific internal IT measures relating directly to VIEW, CCPS and PIPS that are reported in the Balanced Scorecard. For each of these systems it was found that there are measures relating to the system's availability. It was noted, however, that DVA has not developed specific IT measures relating to other business processes that support VIEW, CCPS and PIPS, such as the time taken to process changes requests relating to these systems.

3.15 DVA advised that its Balanced Scorecard already included some IT performance measures in addition to the several service delivery measures for Income Support and Compensation processing. From a client service delivery perspective, DVA believed that adding further IT items to the suite of scorecard measures that measured compensation delivery performance would do little to enhance the value of the scorecard. DVA considered that some lower level of reporting may be more appropriate for monitoring additional IT performance measures.

3.16 The ANAO could not identify a clear linkage between all internal IT measures included in the Balanced Scorecard and related client performance reporting requirements for Income Support and Compensation. In other words, presently there is a 'gap' between the quality and performance standards DVA has with clients and the development of related internal IT measures. This issue is more fully addressed in Paragraphs 6.2 to 6.13.

Information technology architecture

3.17 DVA's information architecture refers to the creation and maintenance of a business information systems model that best organises its information systems. The IMU has responsibility for maintaining the information model. In examining this area, the ANAO sought to establish whether DVA's documented model of its information architecture:

- adequately defined the functions of all appropriate systems;
- was documented, maintained and appropriately communicated; and
- clearly assigned ownership of data and related access rules.

3.18 The ANAO found that documentation of the current model of DVA's information architecture was substantially incomplete. Given the dynamic nature of DVA's Income Support and Compensation related systems, changes and revisions to all relevant documentation should occur promptly.

3.19 By not maintaining current documentation of all aspects of the information systems model, there are increased risks that:

- changes are made to the information systems model that are inconsistent with information technology plans;
- associated costs and risks may not be accurately identified; and
- responsibilities—such as system changes—cannot be effectively discharged.

3.20 The ANAO notes that DVA is currently documenting its information architecture.

Management of IT expenditure

3.21 The ANAO assessed against CobiT criteria the processes underlying DVA's management of its IT expenditure by establishing whether:

- an IT budget process existed and was consistent with DVA's other budget processes;
- there was appropriate IT management involvement in the budgetary process; and
- a process existed for monitoring and controlling actual costs.

3.22 The ANAO found that:

- the overall, higher level allocation and monitoring of IT funding to business areas was consistent with DVA's overall budgeting process;
- business area management confirmed their participation and involvement in the budgeting process; and
- policies and procedures exist to provide guidance and direction for regular monitoring and comparison of actual and budgeted costs.

Communication of the aims and directions of DVA's IT to staff

3.23 In examining the communication of management aims and direction for DVA, the ANAO reviewed whether:

- a framework and awareness program existed that considered integrity, ethical values, codes of conduct, security and internal controls and accountability;
- the framework was consistent with other programs of the organisation;

- senior management promoted a positive control environment by example; and
- senior management has accepted responsibility for developing a framework for the overall approach to IT security.

3.24 The ANAO concluded that an appropriate framework existed that considered integrity, ethical values, codes of conduct, security and internal controls and accountability. At the highest level, the framework was supported by DVA's Corporate Planning statement. This statement promotes core values including integrity, honesty, fairness and openness. IT specific areas were identified including a policy and security framework that also promoted integrity, ethical values and accountability.

3.25 DVA's commitment to its values is evidenced by the prominence of these behaviours in DVA's Corporate Plan. The ANAO found that this reinforced and evidenced senior DVA management's commitment to a positive control environment.

3.26 The ANAO also concluded that senior DVA management, through establishing a structure for key decisions on the department's IT, has formally accepted responsibility for maintaining and communicating integrity, ethical values and a framework for IT security.

Assess risks

3.27 The process of assessing and managing risks is concerned with ensuring the achievement of IT objectives and responding appropriately to threats to the provision of IT services. The assessment and managing of risk is not an IT-specific process. However, the identification, analysis, treatment and monitoring of IT related threats to DVA's assets requires the expertise and advice of the department's IT staff. This expertise and advice ensures specific IT threats and risks can be identified and managed in the context of the overall management of risk at DVA.

3.28 The ANAO sought to establish whether management had implemented an effective overall risk management process that included:

- a systematic risk framework and approach;
- regular revisions;
- consistency with and consideration of organisation-wide objectives; and
- the formal acceptance of any residual risk.

3.29 The ANAO found that DVA has developed comprehensive risk plans across a number of areas, including individual programs, fraud and field operations. At the time of the audit an overall risk assessment and management framework had been adopted and endorsed by senior management.[4]

3.30 In addition, DVA had recently developed and communicated a comprehensive 'Risk Management Policy' that aims to communicate this consistent and rigorous risk management framework and approach to DVA staff. The ANAO concluded that the framework was systematic, allowed for regular revision, was consistent with established approaches to risk management, and it had considered the goals of the department.

Managing quality

3.31 The process of managing the quality of IT systems development, maintenance, operations and documentation is concerned with ensuring the achievement of IT customer requirements. The ANAO sought to establish whether management had implemented an effective quality assurance process within IMU.

3.32 The department had obtained formal accreditation of its IT quality management procedures against internationally recognised standards for quality management.[5] In addition, DVA had adopted an industry-recognised system development life cycle methodology for development and maintenance of its IT systems. The ANAO noted some inconsistencies in DVA's quality management in the areas of quantification of errors, compliance and consistency in the evaluation of errors, timely reporting of quality assurance reports, and the level of critical errors. These concerns were brought to the attention of DVA.

---

4 According to the Australian/New Zealand Standard on Risk Management – AS/NZS 4360:1999 *Risk Management*—risk management is a logical and systematic method of identifying, analysing, evaluating, treating, monitoring and communicating risks associated with any activity, function or process in a way that enables the organisation to minimise losses and maximise opportunities. Risk management is as much about identifying opportunities as avoiding or mitigating losses. The Australian/New Zealand Standard on Risk Management also states that it is the responsibility of management to define and document its risk management framework and to ensure that risk management strategies are understood and implemented at all levels of the organisation.

5 It was consistent with ISO 9001:1994. This document is titled *Standards for Quality Management Systems*, and is developed by the International Standards Organisation and adopted by Standards Australia.

Conclusion

3.33 The ANAO concluded that DVA had in place sound planning and organisation systems and structures and that therefore it met those CobiT process and control objectives for IT planning and organisation applied in this audit.

4. Developing and Maintaining IT Procedures and Managing Change

This chapter reviews DVA's framework for developing and maintaining IT procedures relating to the three systems included in this audit, and DVA's change control procedures for these systems.

4.1 The CobiT domain *Acquisition and Implementation* includes process and control objectives relating to the development and maintenance of IT procedures, and the management of change. The ANAO selected these two process and control objectives as important to the overall governance of IT, and which address the audit's objectives. IT procedures ensure consistent controls are in place and followed. Appropriate management of changes to IT systems ensures that the quality of the IT system is maintained. Together these objectives address system controls and the quality and service delivery parameters set by the department. Table 3 below summarises the conclusions reached against these objectives.

Table 3

Control Objectives for Information and Related Technology Process and Control Objectives—Acquisition and Implementation.

CobiT Process and Control Objectives		*Information criteria*[1]							*Rating*[2] *Scope*		
		Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	S'factory/Recomm	Not in scope[3]	Report Reference
	Acquisition and implementation										
AI1	Identify solutions	P	S							N	
AI2	Acquire and maintain application software	P	P		S		S	S		N	
AI3	Acquire and maintain technology architecture	P	P		S					N	
AI4	Develop and maintain IT procedures	P	P		S		S	S	✓		4.2
AI5	Install and accredit systems	P			S	S				N	
AI6	Manage changes	P	P		P	P		S	R		4.5
	Acquisition and implementation overall								✓		

Notes to table:

1 P = a primary criteria addressed by the objective, S = secondary, a blank cell indicates the objective does not address the information criteria.

2 R indicates an ANAO recommendation.

3 Within time and cost constraints, the ANAO concentrated on controls critical to DVA's business.

Developing and maintaining IT procedures

4.2 Clearly defined procedures are essential to ensure the efficient and effective execution of any process. Computer applications and technological solutions are no exception. Procedures are enabled by a structured approach to the development of user and operations procedure manuals and related training requirements. The ANAO sought to establish whether DVA adopted a sound and structured approach to the development of user and operations procedures and training by considering whether:

- user and operations procedures were documented for the VIEW, CCPS and PIPS systems and kept current;
- service levels and processing requirements were considered when planning for VIEW, CCPS and PIPS system changes; and
- operational requirements were determined with reference to historical performance statistics and appropriate user views.

4.3 The ANAO examined the procedures for developing and using the IT that supports the three applications. Those procedures and documentation involved:

- system designs;
- VIEW, CCPS and PIPS technical system guides;
- the security and availability of technical specifications;
- the IT support requirements for VIEW, CCPS and PIPS; and
- user approval of system specifications.

4.4 The ANAO found that user, operational and technical procedures had been documented and adequately maintained. These procedures were also found to address adequately existing service levels and operational requirements.

Managing changes

4.5 The effective management of system changes is essential to minimise the likelihood of disruptions, unauthorised alterations and errors to the IT systems that support DVA's business. Significant changes occur to DVA's IT systems that support its business processes at least four times per year, with emergency changes also undertaken where necessary. This process consumes significant resources, and is inherently an area of high risk with its potential for introducing errors into the system. For these reasons, the ANAO considers the management of change at DVA to be one of its most critical IT and business processes. The ANAO reviewed DVA's approach and processes for managing IT

system change across most business and compliance areas. In particular, it assessed the effectiveness of DVA's management of changes to the VIEW, CCPS and PIPS systems.

4.6 Recent improvements in DVA's change management processes were identified including the use of new software to improve and centralise change control procedures to ensure a consistent approach across all areas. DVA advised that change requests for CCPS are ranked and balanced against that system's maintenance and development program. Decisions to implement any change take into account the overall workload and competing priorities and their impact. Any delays were a reflection of business decisions on priorities against available resources. Therefore, DVA argued the time taken to implement changes was not a good measure of the efficiency of the change process. DVA drew a distinction between a change that has a major impact and a change that the initiator may consider to be major from a narrow local perspective.

4.7 DVA's change management process was considered to be satisfactory. However, issues were identified relating to the timeliness of change requests, where several change requests for CCPS classified as major had not been actioned for over six months. If major changes are not being actioned on a timely basis, there could be an adverse impact on quality and timeliness of processing resulting in sub-standard performance.

Conclusion

4.8 Overall, DVA's IT procedures were adequately documented and maintained, and the change control process was satisfactory.

Recommendation No.1.

4.9 The ANAO recommends that DVA monitor the time taken to implement changes of its application software, from initiation of a change to its execution, to help ensure all changes which have a significant impact on the business are completed in a timely manner.

DVA Response

4.10 Agreed. However, it must be acknowledged that the department has a project management methodology, appropriate project management procedures and compensating management controls established for some time. These controls are used to ensure that the department is not exposed to unnecessary risk.

5. Delivery and Support

This chapter reports the results of reviews of DVA's management of its IT delivery and support, how DVA ensured uninterrupted IT service, system security and cost attribution, and how DVA managed IT problems and incidents.

5.1 The CobiT domain *Delivery and Support* addresses the IT process and control objectives relevant to IT delivery and support. It will be recalled that an audit objective was to determine whether the three IT systems met quality and service delivery parameters set by the department. Therefore, this CobiT domain was especially relevant to the audit. Table 4 below summarises the objectives of this domain.

Table 4

Control Objectives for Information and Related Technology Process and Control Objectives—Delivery and Support.

CobiT Process and Control Objectives		Information criteria[1]							Rating[2] Scope		Report Reference
		Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	S'factory/Recomm	Not in scope[3]	
Delivery and support											
DS1	Define service levels	P	P	S	S	S	S	S		N	
DS2	Manage third party service	P	P	S	S	S	S	S		N	
DS3	Manage performance and capacity	P	P			S			✓		5.3
DS4	Ensure continuous service	P	S			P			✓		5.8
DS5	Ensure systems security			P	P	S	S	S	✓		5.12
DS6	Identify and attribute costs		P					P	✓		5.20
DS7	Educate and train users	P	S							N	
DS8	Assist and advise IT customers	P								N	
DS9	Manage the configuration	P				S		S		N	
DS10	Manage problems and incidents	P	P			S			✓		5.22
DS11	Manage data				P			P		N	
DS12	Manage facilities				P	P				N	
DS13	Manage operations	P	P		S	S				N	
Delivery and support overall									✓		

Notes to table:

1 P = a primary criteria addressed by the objective, S = secondary, a blank cell indicates the objective does not address the information criteria.

2 R indicates an ANAO recommendation.

3 Within time and cost constraints, the ANAO concentrated on controls critical to DVA's business.

5.2 In order for DVA to deliver services to its clients, the necessary support processes must exist and operate effectively. For DVA, such support processes are driven from the mainframe computing facilities operated by DVA's service provider IBM Australia/IBM GSA. This support includes data processing, which, in turn, includes controls over data entry and reporting for VIEW, CCPS and PIPS.

Manage performance and capacity

5.3 Management of IT performance and capacity requires information on system workload, the size of computer applications, IT resources and demand for computer processing. In regard to these the ANAO determined whether DVA had:

- identified IT performance requirements, targets and standards;
- monitored and reported actual IT system performance including its availability;
- managed those services provided by the principal contractor, IBM Australia and IBM GSA; and
- forecast future IT system requirements and acted on this information.

5.4 The ANAO found that IT system availability, performance and capacity requirements were managed by a process driven by DVA's business needs. Applications, such as VIEW, CCPS and PIPS, were found to drive the capacity planning and performance reporting process sponsored by the department's Information Management Unit. DVA's Business and Infrastructure Team convert these needs into availability measures and requirements. Therefore, DVA had identified its IT performance requirements.

5.5 Monthly performance reporting on central processing unit (CPU) utilisation trends, disk storage trends, availability statistics and many other performance measures are prepared and disseminated to business areas for review and action. DVA had a service level agreement with its principal IT service provider to assist with the monitoring of resource availability requirements for DVA IT systems.

5.6 DVA monitored its utilisation of its computer processing on IBM's central computers. Recording of business critical events and related action occurred as part of this process. Also, the department had a contract manager for its contract and service level agreement with its principal IT service provider. The department also considered data and system security issues in its contract management. In other words, DVA regularly reviewed reports on the performance and capacity of VIEW, CCPS and PIPS.

5.7 Overall, DVA:

- identified its IT performance requirements;
- monitored system performance including its availability;
- managed those services provided by its principal contractor; and
- forecast future IT system requirements and acted on this information.

Ensuring continuous service

5.8 For DVA to achieve the outputs and outcomes determined for it by the Government and encapsulated in its corporate plan, IT services must be available as required and continue in the event of a disaster. Ideally, this availability should be enabled by developing, implementing and testing disaster recovery, contingency and continuity plans that address IT and business aspects. The ANAO considered DVA's performance in this area by considering whether:

- an IT continuity framework existed that defined the roles, responsibilities and risks;
- a written plan existed with procedures for:
  - emergencies;
  - recovering and responding to bring back the business to its state prior to the incident;
  - communicating with stakeholders such as employees, customers and suppliers;
  - safeguarding sites and personnel; and
  - information on continuity personnel and affected stakeholders,
- the IT continuity plan was maintained;
- the IT continuity plan was tested; and
- appropriate IT continuity training, distribution, back up and administration occurred.

5.9 The ANAO found that a written IT continuity framework existed with key factors identified for the effective management of this process. The IT business continuity plan training, distribution, back-up and administration were also found to be satisfactory. The business continuity plan was developed to cover, operational, administrative and accommodation requirements in the event of a disruption to essential services. A key component of the business continuity plan relates to the restoration of IT services and facilities. The business continuity plan was revised and tested as part of Year 2000 preparations.

5.10 The business continuity plan includes a emergency contact list for IT Systems and communication contained within an appendix. This list is the same as the list for 'Emergency Situations' as listed in the 'DVA / IBM GSA Escalation and Notification Procedures' Guideline. As well as being published, the business continuity plan is available on the DVA intranet.

5.11 Overall, DVA's process for ensuring continuous service from VIEW, CCPS and PIPS was found to be satisfactory.

Ensuring systems security

5.12 A further CobiT process and control objective is systems security. Systems security is concerned with safeguarding against unauthorised use, disclosure, modification, damage or loss of information that is stored, disseminated and maintained by the department's IT systems. The ANAO sought to assess the efficiency and effectiveness of DVA's performance against this area by considering whether logical access controls existed that ensured access to VIEW, CCPS and PIPS. The ANAO also assessed whether access to data and programs supporting the Income Support and Compensation business processes was restricted to authorised users. Logical access controls are controls that determine the applications that individuals can access, once access to a physical terminal is available to the individual.

5.13 The ANAO considered this control objective at two levels: first, logical access to the underlying infrastructure (mainframe and related areas); and, second, the effectiveness of logical access security to VIEW, CCPS and PIPS specific programs and related IT systems. The ANAO then assessed DVA's performance in this area by determining whether there was:

- appropriate control over logical access to resources supporting VIEW, CCPS and PIPS;
- regular monitoring of user access and changes to access rights; and
- an appropriate security incident handling procedure established.

5.14 In regard to the first level of logical access to the underlying infrastructure, DVA had a number of integrated systems that work together to provide a secure IT environment. The ANAO focused on the security systems that affected the IT systems supporting the VIEW, CCPS and PIPS. These systems were Windows NT and ACF2. Windows NT is the entry point to DVA's systems, while ACF2 is used as the password validation resource for all mainframe services. The main functions were found to be:

- user account management (user creation, deletion, suspension and activation);
- uniform security management across all major platforms;
- one common interface to security management; and
- provision of an on-line security request and approval process.

5.15 The ANAO found that there was limited event logging performed on the Windows NT environment. By not utilising the Windows NT event logging, there is an increased risk that business rules for access are breached without detection on timely basis. Also, the efficiency benefits from Windows NT event logging may not be fully realised. Notwithstanding, there was appropriate overall control over logical access to resources supporting the three main applications included in this audit.

5.16 The second level of systems security considered here was the effectiveness of logical access security to the three specific programs and related IT systems. Inadequate reviews were performed of records of access to the program that, in turn, permitted access to computer code and computer-stored data. Those records of access are called audit logs[6]. Without formal procedures for review of audit logs, users in a position of trust can breach their authority and responsibility without detection.

5.17 The ANAO also reviewed logical access to information resources by personnel in the relevant Income Support and Compensation business areas. Test procedures undertaken as part of the financial audit of DVA found logical access to VIEW, CCPS and PIPS resources by business area personnel to be adequately controlled.

5.18 The management of DVA's IT system security, including Windows NT and ACF2 applications, was satisfactory. However, the systems could also be improved by effectively logging events performed in the Windows environment and reviewing records of access to programs.

5.19 DVA advised that an event logging system was in place, and regular reviews of audit logs were performed. DVA also advised that it continuously improved security counter measures to mitigate against unauthorised access.

---

[6] The computer program that permitted read access to computer data and code was called ObjectStar workbench.

Identifying and attributing costs

5.20 Cost justification, in the context of this audit, means identifying the cost of delivering the service provided by the three systems examined in this audit, and justifying the expense of that service. Information on IT costs is a part of the costs of the department's production of its outputs and outcomes. Such information can also be used by the department to compare its production costs with those of other agencies in the public and private sectors.

5.21 Subsequent to the fieldwork of the audit DVA advised that there are three levels for measuring the unit cost for processing claims and reviews, and one of these is the complete cost of service delivery. This includes a relevant proportion of the cost of providing the key IT systems, such as CCPS, PIPS and VIEW, which support the relevant business processes. DVA recently conducted an Output Pricing Review exercise for DOFA which included high level benchmarking of DVA business processes with similar processes in other agencies. The comparison of unit costs for service delivery to pensioners included the cost of IT provision.

Managing IT problems and incidents

5.22 The ANAO reviewed DVA's management of IT problems and incidents at two levels: first, management of problems and incidents affecting the underlying infrastructure (mainframe and related areas); second, management of problems and incidents affecting VIEW, CCPS and PIPS and related IT systems. The ANAO determined whether:

- an effective problem management process and system existed;
- problem escalation procedures existed to ensure the effective resolution of identified problems and incidents; and
- adequate problem tracking existed and sufficient audit trails were maintained and retained for system problems.

5.23 DVA has a problem and incident management process, including escalation procedures, that are supported by guidelines between DVA and its principal service provider[7], and by specialist software[8]. Through the use of its specialist software, DVA records, analyses, ranks, takes action on and reports problems and incidents and their resolution in an effective manner. Therefore, an effective problem management process and system existed.

---

7 This is the 'DVA/IBM GSA Escalation and Notification Procedures' Guideline.

8 This software is called CrossView.

5.24 The contract with the principal IT service provider established an all hours customer care management centre as a first point of contact for DVA officers when they need assistance. Further information for departmental staff on responses to IT problems is available on the departmental intranet. The department and the principal IT service provider apply procedures, including escalation procedures, for addressing IT problems and incident management.

5.25 DVA's management of problems and incidents was found to be satisfactory at both the infrastructure-operations level, and for the VIEW, CCPS and PIPS system directly supporting the Income Support and Compensation business processes. In other words, adequate problem escalation procedures existed, adequate problem tracking existed, and audit trails were maintained and utilised.

Conclusion

5.26 Overall DVA had identified its IT performance requirements; ensured continuous service from the three systems reviewed; had adequate systems security; had undertaken work to identify the costs of its IT operations; and had managed problems and incidents satisfactorily.

6. Monitoring

This chapter reports the results of ANAO's review of DVA's monitoring of its IT.

6.1 A key audit objective was to identify sound practice and any deficiencies in the IT controls of the three systems and any effect on the department's operations. A relevant CobiT domain was monitoring of IT systems. Monitoring included, as well as DVA's monitoring of its IT processes, the department's assessment of the adequacy of its internal controls, whether the department had obtained independent assurance of its systems, and whether its systems were audited independently. Table 5 below summarises the CobiT objectives and the ANAO's conclusions against those findings.

Table 5

Control Objectives for Information and Related Technology Process and Control Objectives—Monitoring

CobiT Process and Control Objectives		*Information criteria*[1]							*Rating*[2] / *Scope*		Report Reference
		Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	S'factory/Recomm	Not in scope[3]	
	Monitoring										
M1	Monitor the process	P	S	S	S	S	S	S	R		6.2
M2	Assess internal control adequacy	P	P	S	S	S	S	S	✓		6.22
M3	Obtain independent assurance	P	P	S	S	S	S	S	✓		6.24
M4	Provide for independent audit	P	P	S	S	S	S	S	✓		6.26
	Monitoring overall								✓		

Notes to table:

1 P = a primary criteria addressed by the objective, S = secondary, a blank cell indicates the objective does not address the information criteria.

2 R indicates an ANAO recommendation.

3 Within time and cost constraints, the ANAO concentrated on controls critical to DVA's business.

Monitoring the processes

6.2 It is important for management to monitor IT processes in order to determine if those processes are achieving their objectives. IT monitoring requires management to define reporting and performance indicators, to implement supporting systems and to act on reported results. The ANAO assessed the performance of DVA in this area by considering whether DVA had:

- identified key performance indicators to measure IT system performance; and
- implemented adequate internal and external IT systems reporting for both IT users and non-IT users such as clients, senior management and external auditors.

Identifying Key Performance Indicators for IT system performance

6.3 Departmental Income Support and Compensation staff require a common understanding of the level of service to be provided by the VIEW, CCPS and PIPS systems. Such an understanding is enabled by the setting and publicising of IT system service levels. The ANAO reviewed the appropriateness of IT system service levels and related reporting.

6.4 The ANAO found that DVA's arrangements, as they related to targets and reporting, were satisfactory. In addition, the ANAO found that internal system performance measures relating to these areas were satisfactory. However, DVA did not have a clear, documented linkage between these internal IT system performance measures and client quality and performance targets reported in the Balanced Scorecard for Income Support and Compensation. This matter was first raised in Chapter 3.

6.5 The client quality and performance targets included:

- number of income support new claims processed;
- target of 19 days to process a Pensioner Initiated Review (PIR);
- fewer than 5 per cent critical errors for Income Support Payments;
- results of Veteran Satisfaction Survey;
- target of 75 days to process a primary claim;
- less than 5 per cent critical error for Compensation Claims;
- average cost per primary claim;
- target for processing compensation appeals reports; and
- average cost per review activity.

6.6 DVA's internal audit program regularly identifies informal internal control targets relating to these areas and reports performance by the IT systems against these targets. This internal audit activity could be a suitable basis for the department to develop a control framework for the operations areas to implement. In addition, the CobiT framework could be used by the department as a basis for the development of appropriate internal IT system control targets.

6.7 The ANAO also identified relevant internal IT system control targets relating to these areas and assessed actual performance against them. Specific IT systems targets supporting VIEW, CCPS and PIPS that were examined as part of the ANAO's annual financial audit included:

- completeness, validity, timeliness and accuracy of IT system inputs, data processing and system outputs;
- effectiveness of change management and problem management processes for the IT systems;
- effectiveness of IT systems security; and
- effectiveness of IT systems detective controls, including compliance systems and programs.

6.8 The ANAO financial statement IT audit found how its testing indicated that moderate reliance could be placed on the systems and controls and accuracy of the accounts and records. Moderate reliance means that the IT controls are sound and operating effectively, and that the sample size in the financial audit substantive testing can be reduced.

6.9 DVA advised that it generates reports on system outage times for a number of key IT systems, including VIEW, CCPS and PIPSPC, and that these are included in the Balanced Scorecard. Staff were working towards being able to provide system availability figures for these systems (expressed as a percentage of core time). It was also intended to include an indication of targets when reporting system availability figures. The current report included a financial summary of support projects, including VIEW, CCPS and PIPSPC. DVA indicated that there may be merit in reviewing its system model documentation, and that all proposals for improving its management in this area would be addressed on a cost-benefit basis. DVA further indicated that the Balanced Scorecard includes some IT infrastructure measures. These include system availability for key IT business systems. There were also measures for the number of IT system problems reported, and the percentage of outstanding problems resolved in a given quarterly period.

6.10 The ANAO noted that acceptable performance variations from IT system targets—both internal and external—had not been developed.

6.11 The ANAO notes that the department is planning to benchmark aspects of its operations against other similar schemes. In particular DVA's income support processing will be compared with Centrelink.

Recommendation No.2.

6.12 The ANAO recommends that DVA:

- formulate IT Balanced Scorecard measures that directly link, and relate to, relevant IT strategy statements. These measures would then enable effective monitoring of progress in implementing the IT strategic plan;
- develop suitable measures for IT systems that support DVA's client performance reporting requirements;
- review and update the information systems model documentation to ensure it is complete and current to facilitate operations and any changes that may be required;
- clearly articulate in its balance scorecard reports:
  - inherent limitations on the accuracy of performance reports; and
  - clear explanations and definitions of key terms used in the reports, including what is meant by 'error' and 'accuracy'; and
- formalise acceptable variations from agreed targets for all internal and external IT system reporting.

DVA's Response

6.13 Agreed. However, it must be acknowledged that the department's Balanced Scorecard methodology has been evolving since it was established. The methodology is continuously improved to include a range of suitable performance measures including IT activities that directly link, relate to and report on relevant IT strategy statements.

Reporting against Key Performance Indicators

6.14 The effective reporting of IT system performance against service levels should ensure that a consistent, overall process exists for:

- identifying what relevant information is to be captured;
- determining the regularity of reporting;
- ensuring the consistency of reporting;
- reporting on unanticipated events; and
- monitoring and follow up.

6.15 The ANAO assessed DVA's performance in this area by reviewing reporting against service levels and Balanced Scorecard targets for VIEW, CCPS and PIPS and related business processes. The ANAO concluded that DVA monitored its IT system performance, capacity, and service level agreements.

Continuous improvement program

6.16 DVA has implemented a Continuous Improvement Program to assist it to improve its delivery of services. Previously, DVA's internal reporting was mainly focused on agreed client targets: that is, non-IT specific but IT-dependent indicators. This reporting did not include data on the performance of the IT systems, but data on items such as payment accuracy and timeliness. Other reporting to customers includes the results of a regular Veterans' Satisfaction Survey.

6.17 Recently IT performance reporting has included IT measures on:

- IT system down time;
- IT system availability;
- number and grade of IT systems or environment problems;
- percentage of problems resolved within target times;
- percentage of customer care management centre calls resolved; and
- IT financial performance.

6.18 This IT performance reporting was comprehensive. DVA's Strategic Support Branch, which includes internal audit, coordinates this reporting to departmental output areas and to the Executive Management Group.

6.19 Inherent in this process is the reliance placed on the internal targets developed for IT system effectiveness, efficiency and control by the operations and business process areas. The Balanced Scorecard report to clients, however, does not currently define the context of its preparation and related limitations.

Reporting on accuracy of Income Support and Compensation processes

6.20 The documents resulting from identification of critical errors for Income Support were examined during the financial audit. It was noted that there were instances whereby particular types of errors were

inconsistently categorised. Further, the categorisation of errors and the sampling techniques used to selected records were subjective, and therefore the classification may not be consistent across all DVA state offices. DVA does not quantify critical errors to determine the magnitude of errors over total payments. It is noted that DVA is currently conducting undertaking a review of its quality assurance process (the Quality Assurance Enhancement Project—Income Support) to address these issues.

6.21 These are considered significant limitations to the level of assurance able to be provided by DVA to its clients on the accuracy of the delivery of Income Support and Compensation by the IT systems and related processes.

Assessing the adequacy of internal control

6.22 The ANAO assessed whether DVA:

- continuously monitored controls over its IT and business processes; and
- reported regularly to management on the effectiveness and efficiency of internal controls.

6.23 Internal review and oversight of external review activity is the responsibility of the National Audit and Fraud Committee (NAFCOM). NAFCOM meets quarterly and it is chaired by the Deputy President of the Repatriation Commission. NAFCOM considers all review and audit reports, including all IT reviews. This indicated a strong commitment to management support and monitoring of internal controls.

Independent assurance

6.24 Independent assurance is an approach to providing for an increased level of confidence in the system being used by an organisation. It is enabled by independent assurance reviews carried out at regular intervals. The ANAO assessed whether DVA management had implemented an assurance process that, amongst other things, included its IT systems. The ANAO then assessed whether that assurance process considered:

- independent certification and accreditation;
- independent effectiveness evaluations;
- performance of assurance reviews by qualified personnel; and
- audit involvement.

6.25 The ANAO found that DVA had obtained independent accreditation[9] for the IMU's quality management system. Independent accreditation includes evaluation of the IMU's effectiveness, and it is conducted by independent, qualified personnel. This, together with the level of independent and active internal and ANAO review, led to the conclusion that DVA had an appropriate independent assurance process for management of its outsourced IT systems.

Provide for independent audit

6.26 The ANAO considered, in relation to DVA's IT function:

- audit independence;
- active audit involvement;
- performance of audits by qualified personnel; and
- clearance of findings and recommendations.

6.27 DVA's Strategic Review Services group incorporates a number of functions including internal audit, IT audit, risk management and evaluation. DVA has entered into a partnering arrangement with the private sector for provision of these services. The ANAO found:

- internal audits are conducted in accordance with appropriate standards;
- the organisational status of the Strategic Review Services group appeared to support the unbiased forwarding of audit results to the National Audit and Fraud Committee; and
- the scope of the internal audit function appeared complete in that there is a planned approach to ensure coverage of key areas, with flexibility to include ad-hoc topics in the audit plan.

6.28 The Strategic Review Services group is also responsible for the development and implementation of a monitoring program that consolidates, reviews and clears findings from internal and financial statement audits.

---

9 ISO 9001:1994. This is the international standard for quality management systems, as developed by the International Standards Organisation and adopted by Standards Australia.

6.29 The ANAO conducts an audit of DVA's financial statements each year. That annual audit has a major IT audit component. In addition, the ANAO conducts a small number of performance audits of DVA each year. Most of these performance audits include a component that considers some IT aspects of DVA's performance. As stated above, ANAO audit reports are provided to DVA's Executive, the Minister for Veterans' Affairs and to the National Audit and Fraud Control Committee.

Conclusion

6.30 Overall, DVA's internal system performance measures were satisfactory. DVA monitored its system performance, and the department had adequate independent assurance for its systems. However, acceptable performance variations from IT system targets had not been developed for performance management purposes.

Canberra ACT
5 June 2001

P. J. Barrett
Auditor-General

Appendices

Appendix 1

Description of the Three IT Systems Reviewed in this Audit

Veteran Information Enquiry Window (VIEW)

VIEW is a PC based enquiry window that consolidates all client information into one application. It provides a plain English inquiry facility that allows examination of information held on the department's clients. The VIEW platform includes client registration (replacing the previous Client Registration System), and it can access the new Integrated Payment System (IPS). Information is presented in a graphical format and is easy to find and understand, due in part, to the conversion of codes to plain English. The client registration facility includes the additional functionality of issuing a unique identification number for every client record created. VIEW is accessible at both State and National level.

Pension Information Processing System (PIPS)

PIPS runs on DVA's local area network in each state office. Client financial and personal details are retrieved from the client database held on the central computer and stored on a temporary worksheet on the local network. This information is then updated and held locally. The information is transferred daily to update the central computer record. The information is used to calculate:

- service pensions;
- disability pensions;
- income support supplements; and
- lump sum advance payments.

Compensation Claims Processing System (CCPS)

Departmental claims assessors use CCPS when assessing the compensation claims of war veterans. The system operates on the local network in each state office retrieving information from the central computer client database. Claims assessors use CCPS for assessing claims for:

- disability pension;
- increases in disability pensions;
- other assessment/reviews of disability pension; and
- claims for war widows pensions in respect of the death of a veteran.

Appendix 2

CobiT: Control Objectives for Information and Related Technology

CobiT EXECUTIVE OVERVIEW[10]

Critically important to the success and survival 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. Truly, information and information systems are pervasive throughout organisations—from the user's platform to local and wide area networks to client servers to mainframe computers. Thus, 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. Thus, management needs to have an appreciation for and a basic understanding of the risks and constraints of IT in order to provide effective direction and adequate controls. CobiT helps bridge the gaps between business risks, control needs and technical issues. It provides good practices across a domain and process framework and

---

[10] This Executive Overview is taken from the CobiT Executive Summary, April 1998 2nd Edition. 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.

presents activities in a manageable and logical structure. CobiT's 'good practices' means consensus of the experts—they will help you optimise your information investment, but foremost they are what you will be judged upon when things do go wrong.

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 establish an adequate system of internal control. Thus, an internal control system or framework must be in place to support the business processes and it must be clear how each individual control activity satisfies the information requirements and impacts the 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 management's responsibility. Management, through its corporate 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 not only to be employed by users and auditors, but also, and more importantly, as a comprehensive checklist for 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.

It continues with a set of 34 high-level Control Objectives, one for each of the IT processes, grouped into four domains: planning & organisation, acquisition & implementation, delivery & 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. In addition, corresponding to each of

the 34 high-level Control Objectives is an audit, or assurance, guideline to enable the review of IT processes against CobiT's 302 recommended detailed control objectives to provide management assurance and/or advice for improvement. CobiT contains an *Implementation Tool Set* which provides lessons learned from those organisations that quickly and successfully applied CobiT in their work environments. It includes an Executive Summary for senior management awareness and understanding of CobiT's key concepts and principles. The implementation guide has two useful tools—Management Awareness Diagnostic and IT Control Diagnostic—to assist in analysing an organisation's IT control environment.

The management of the organisation needs generally applicable and accepted IT governance and control practices to benchmark their existing and planned IT environment. CobiT is a tool that allows managers to communicate and bridge the gap with respect to control requirements, technical issues and business risks. CobiT enables the development of clear policy and good practice for IT control throughout organisations, worldwide. It is CobiT's goal to provide these control objectives, within the defined framework, and obtain endorsement from commercial, governmental and professional organisations, world-at-large.

Thus, CobiT is intended to be *the* breakthrough IT governance tool that helps in understanding and managing the risks associated with information and related IT.

Table 6 below lists the full range of CobiT process and control objectives and the information criteria that they address.

Table 6

Overview of CobiT objectives and the criteria that they address.

CobiT Process and Control Objectives		*Information criteria*[1] (P= primary, S= Secondary)						
		Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
	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	S	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						
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		

CobiT Process and Control Objectives		*Information criteria*[1] (P= primary, S= Secondary)						
		Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
Monitoring								
M1	Monitor the process	P	S	S	S	S	S	S
M2	Assess internal control adequacy	P	P	S	S	S	S	S
M3	Obtain independent assurance	P	P	S	S	S	S	S
M4	Provide for independent audit	P	P	S	S	S	S	S

Note to table

1 A blank cell indicates the objective does not address the information criteria.

Index

Series Titles

Titles published during the financial year 2000–01

Audit Report No.43 Performance Audit
Performance Information for Commonwealth Financial Assistance under the National Heritage Trust
Department of Agriculture, Fisheries and Forestry, Department of the Environment and Heritage

Audit Report No.42 Performance Audit
Bank Prudential Supervision
Australian Prudential Regulation Authority

Audit Report No.41 Performance Audit
Causes and Consequences of Personnel Postings in the Australian Defence Force
Department of Defence

Audit Report No.40 Performance Audit
Management of the Adult Migrant English Program Contracts
Department of Immigrationand Multicultural Affairs

Audit Report No.39 Performance Audit
Information and Technology in Centrelink
Centrelink

Audit Report No.38 Performance Audit
The Use of Confidentiality Provisions in Commonwealth Contracts

Audit Report No.37 Performance Audit
The Use of Audit in Compliance Management of Individual Taxpayers
Australian Taxation Office

Audit Report No.36 Performance Audit
Municipal Services for Indigenous Communities
The Aboriginal and Torres Strait Islander Commission

Audit Report No.35 Performance Audit
Family and Community Services' Oversight of Centrelink's Assessment of New Claims for the Age Pension
Department of Family and Community Services

Audit Report No.34 Performance Audit
Assessment of New Claims for the Age Pension by Centrelink
Centrelink

Audit Report No.33 Performance Audit
Australian Defence Force Reserves
Department of Defence

Audit Report No.32 Performance Audit
Defence Cooperation Program
Department of Defence

Audit Report No.31 Performance Audit
Administration of Consular Services
Department of Foreign Affairs and Trade

Audit Report No.30 Performance Audit
Management of the Work for the Dole Programme
Department of Employment, Workplace Relations and Small Business

Audit Report No.29 Performance Audit
Review of Veterans' Appeals Against Disability Compensation Entitlement Decisions
Department of Veterans' Affairs
Veterans' Review Board

Audit Report No.28 Audit Activity Report
Audit Activity Report: July to December 2000
Summary of Outcomes

Audit Report No.27 Performance Audit
Program Administration Training and Youth Division—Business Reengineering
Department of Education, Training and Youth Affairs (DETYA)

Audit Report No.26 Performance Audit
Defence Estate Facilities Operations
Department of Defence

Audit Report No.25 Benchmarking Study
Benchmarking the Finance Function

Audit Report No.24 Performance Audit
Family Relationships Services Program (FRSP)
Department of Family and Community Services (FaCS)

Audit Report No.23 Financial Statement Audit
Audits of the Financial Statements of Commonwealth Entities for the Period Ended 30 June 2000

Audit Report No.22 Performance Audit
Fraud Control in Defence
Department of Defence

Audit Report No.21 Performance Audit
Management of the National Highways System Program
Department of Transport and Regional Services

Audit Report No.20 Performance Audit
Second Tranche Sale of Telstra Shares

Audit Report No.19 Financial Control and Administration Audit
Management of Public Sector Travel Arrangements—Follow-up audit

Audit Report No.18 Performance Audit
Reform of Service Delivery of Business Assistance Programs
Department of Industry, Science and Resources

Audit Report No.17 Performance Audit
Administration of the Waterfront Redundancy Scheme
Department of Transport and Regional Services
Maritime Industry Finance Company Limited

Audit Report No.16 Performance Audit
Australian Taxation Office Internal Fraud Control Arrangements
Australian Taxation Office

Audit Report No.15 Performance Audit
Agencies' Performance Monitoring of Commonwealth Government Business Enterprises

Audit Report No.14 Information Support Services Report
Benchmarking the Internal Audit Function

Audit Report No.13 Performance Audit
Certified Agreements in the Australian Public Service

Audit Report No.12 Performance Audit
Passenger Movement Charge—Follow-up Audit
Australian Customs Service

Audit Report No.11 Performance Audit
Knowledge System Equipment Acquisition Projects in Defence
Department of Defence

Audit Report No.10 Performance Audit
AQIS Cost-Recovery Systems
Australian Quarantine and Inspection Service

Audit Report No.9 Performance Audit
Implementation of Whole-of-Government Information Technology Infrastructure Consolidation and Outsourcing Initiative

Audit Report No.8 Performance Audit
Amphibious Transport Ship Project
Department of Defence

Audit Report No.7 Performance Audit
The Australian Taxation Offices' Use of AUSTRAC Data
Australian Taxation Office

Audit Report No.6 Performance Audit
Fraud Control Arrangements in the Department of Health & Aged Care
Department of Health & Aged Care

Audit Report No.5 Performance Audit
Fraud Control Arrangements in the Department of Industry, Science & Resources
Department of Industry, Science & Resources

Audit Report No.4 Activity Report
Audit Activity Report: January to June 2000—Summary of Outcomes

Audit Report No.3 Performance Audit
Environmental Management of Commonwealth Land—Follow-up audit
Department of Defence

Audit Report No.2 Performance Audit
Drug Evaluation by the Therapeutic Goods Administration—Follow-up audit
Department of Health and Aged Care
Therapeutic Goods Administration

Audit Report No.1 Performance Audit
Commonwealth Assistance to the Agrifood Industry

Better Practice Guides

Internet Delivery Decisions	Apr 2001
Planning for the Workforce of the Future	Mar 2001
Contract Management	Feb 2001
AMODEL Illustrative Financial Statements 2000	Apr 2000
Business Continuity Management	Jan 2000
Building a Better Financial Management Framework	Nov 1999
Building Better Financial Management Support	Nov 1999
Managing APS Staff Reductions (in Audit Report No.47 1998–99)	Jun 1999
Commonwealth Agency Energy Management	Jun 1999
Corporate Governance in Commonwealth Authorities and 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
Life-cycle Costing (in Audit Report No.43 1997–98)	May 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
Return to Work: Workers Compensation Case Management	Dec 1996
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