The Auditor-General

Audit Report No.22
Performance Audit

Getting Over the Line

Selected Commonwealth Bodies' Management of the Year 2000 Problem

Australian National Audit Office

ISSN 1036-7632

ISBN 0 644 39137 5

Australian National
Audit Office

Canberra ACT
15 December 1998

Dear Madam President
Dear Mr Speaker

The Australian National Audit Office has undertaken a performance audit of selected Commonwealth bodies 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 *Getting Over the Line – Selected Commonwealth Bodies' Management of the Year 2000 Problem.*

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 7798

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

http://www.anao.gov.au

Audit Team
John Butcher
Lyn Chapman
Colin Cronin

Contents

Summary and Recommendations

Audit Findings and Conclusions

Abbreviations

Airservices	Airservices Australia
ANAO	Australian National Audit Office
APCA	Australian Payments Clearing Association
APRA	Australian Prudential Regulation Authority
ATO	Australian Taxation Office
CES	Commonwealth Employment Service
CGIO	Chief Government Information Officer
CIP	Corporate Information Program
Customs	Australian Customs Service
DAO	Defence Acquisitions Organisation
DCB	Defence Computing Bureau
DCG	Defence Communications Group
DCITA	Department of Communications, Information Technology and the Arts
DEETYA	The former Department of Employment, Education, Training and Youth Affairs (*now the Department of Education, Training and Youth Affairs*)
Defence	Department of Defence
DEFMIS	Defence Financial Management Information System
DEO	Defence Estate Organisation
DETYA	Department of Education, Training and Youth Affairs, formerly the *Department of Employment, Education, Training and Youth Affairs (DEETYA)*. As a result of changes in administrative arrangements announced in October 1998, responsibility for employment services transferred to the new Department of Employment, Workplace Relations and Small Business (DEWRSB). Although this report will refer to the Department by its new name (DETYA, unless otherwise indicated by the context) the findings contained in this report pertain to the former *DEETYA* (including the employment services component).

DEWRSB	Department of Employment, Workplace Relations and Small Business
DFAT	Department of Foreign Affairs and Trade
DIMA	Department of Immigration and Multicultural Affairs
DISR	Department of Industry, Science and Resources
DNSG	Defence Network Services Group
DRP	Defence Reform Program
EAT	External Assurance Testing
EMA	Emergency Management Australia
GAO	General Accounting Office
IT&T	Information Technology (IT) and Telecommunications
IWG	Inter-bank Working Group
NAO	National Audit Office
OECD	Organisation of Economic Cooperation and Development
OGIT	Office of Government Information Technology
OGO	Office for Government Online (formerly OGIT). As a result of changes in administrative arrangements announced in October 1998, OGIT's functions transferred from the Finance and Administration portfolio to the Communications, Information Technology and the Arts portfolio, and was renamed the Office for Government Online.
RBA	Reserve Bank of Australia
SCA	Support Command Australia
SDSS	Standard Defence Supply System
UN	United Nations
US	United States
Y2K	Year 2000

Glossary

applications

term commonly used to refer to specific items of software (for example, a word-processing package is an application).

Commonwealth agencies

in the context of this report, the term *agencies* is used to refer to budget-funded organisations which are subject to the *Financial Management and Accountability Act 1997.*

Commonwealth bodies

generic term used to refer to Commonwealth *agencies* and Commonwealth *entities*.

Commonwealth entities

in the context of this report, the term *entities* is used to refer to off-budget commercial organisations subject to the *Commonwealth Authorities and Companies Act 1997*.

computer programs

a sequence of machine readable instructions designed to perform a predetermined manipulation of data in order to solve a specified problem.

embedded systems

refers to equipment containing microchips and/or firmware; process monitoring, control and data acquisition systems; or any other equipment and/or operating systems used to control the operations of equipment or machinery. Embedded systems are frequently used in manufacturing and building systems and are sometimes referred to as *non-IT*, principally because they are not generally included in the IT inventory.

end-to-end testing

generally used to refer to the testing of external interfaces through which data is transferred between organisations or between business arms of organisations.

integration testing

sometimes used interchangeably with the term *end-to-end testing* and refers to the testing of *interfaces* to ensure the integrity of data transfer between *applications* and/or *systems* which support a business function.

interface

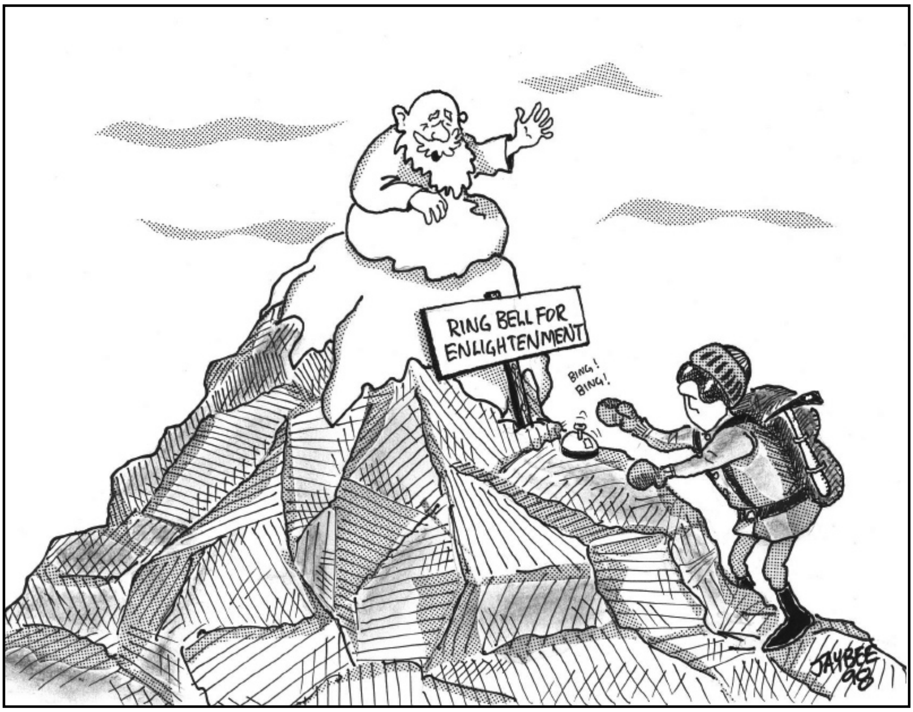
refers to the point of data transfer between *applications* and/or *systems.*

microprocessors — computer chips, or microchips, *embedded* in equipment and which perform functions or calculations necessary to its operation.

systems — commonly refers to an *application* or group of applications linked together (or *integrated*) to perform business functions.

work-arounds — term commonly used in IT to refer to alternative processes or procedures which might be invoked to cope with a systems failure and, in the Year 2000 context, is generally used to refer generally to any fall-back procedure or process used to cope with a failure of a business process or system.

Summary and Recommendations



Year 2000 Strategy? My son, this *IS* my Year 2000 strategy!

Summary

Background

Government services potentially affected by Year 2000 problem

1. The Year 2000 problem refers to the inability of some computer programs and micro processors to recognise or perform calculations using either a four digit year date or a two digit year date where the year 2000 is represented as '00'. This may result in the program failing to operate correctly, either by shutting down or producing erroneous results. The core business functions of Commonwealth bodies are increasingly reliant on information technology and telecommunications (IT&T). The extent of business process automation means that, in the event of any Year 2000 disruption to automated business systems, many Commonwealth bodies may not be able to substitute manual processes without significantly affecting program efficiency and the effectiveness of client services.

Whole-of-business issue, not just an 'IT' problem

2. The Year 2000 problem is a whole-of-business issue, not just an IT problem, and has presented a significant challenge to governments and industry. This means that solutions to the Year 2000 problem require the mobilisation of people and resources across an organisation's operations. The six budget-funded Commonwealth agencies reviewed for the current audit reported total estimated Year 2000 costs of $286.3 million, of which approximately two thirds is accounted for by the Department of Defence.

Previous ANAO audit found that agencies were not well prepared

3. In a previous audit (Audit Report No. 27, 1997-98) the ANAO examined Commonwealth bodies' risk assessment and management of the Year 2000 problem. The audit reported the results of a survey of 74 Commonwealth bodies undertaken in mid-1997. The audit found that the majority of bodies surveyed:

- were unable to provide estimates of the total cost for their organisation to become Year 2000 compliant;

- had not adequately analysed and established priorities for their Year 2000 risks from a whole-of-business perspective;
- were not well advanced in the preparation of inventories of Year 2000 affected products and services; and
- had not undertaken any compliance testing of their systems and applications.

Audit approach

Current audit examined project management, resources and achievement of milestones

4. In view of the significance of the Year 2000 problem for Commonwealth bodies and their clients, a further audit was scheduled to assess, for selected bodies:

- the extent to which recommendations arising from the previous audit have been implemented;
- the extent to which Year 2000 projects demonstrate accepted elements of better practice;
- the application of appropriate financial and human resources to Year 2000 activities and the impact of Year 2000 resource deployment on non-Year 2000 IT and business initiatives;
- progress against accepted Year 2000 project milestones given selected bodies' organisational and operational profiles; and
- confidence levels in relation to: assessment of risks to business critical activities; implementation of risk mitigation strategies; and the likelihood of resolving Year 2000 risks to business critical functions.

Audit reviewed eight Commonwealth bodies providing key Government functions

5. The ANAO undertook field work from June to September 1998 in Commonwealth bodies responsible for the delivery of key government functions, including revenue collection, social welfare, public safety, national security and economic regulation. The bodies examined represent a significant proportion of Commonwealth expenditure and revenue. The eight bodies were: Airservices Australia (Airservices); Australian Customs Service (Customs); Australian Taxation Office (ATO); Centrelink; Department of Defence (Defence); the then Department of

Employment, Education, Training and Youth Affairs (DEETYA, now *DETYA*); Department of Immigration and Multicultural Affairs (DIMA); and Reserve Bank of Australia (RBA). The ANAO also reviewed the Office for Government Online's (OGO, formerly the Office of Government Information Technology, or 'OGIT') whole-of-government coordination of the Commonwealth's Year 2000 efforts.

Audit conclusions

Year 2000 requires strong executive management focus

6. The audit conclusions are drawn from the more significant findings outlined in the audit report. The findings set out in this audit indicate that the Year 2000 problem will continue to require a strong executive management focus. Each Commonwealth body will need to closely monitor and report its progress towards Year 2000 compliance both to ensure effective internal governance and to support monitoring and reporting on a whole-of-government basis. Continuity management planning will become increasingly important for individual Commonwealth bodies and at a whole-of-government level.

Responsibility for compliance rests with individual Commonwealth bodies

7. While OGO has a whole-of-government coordination role in relation to Year 2000 activities, it is the responsibility of the chief executive and/or board of each Commonwealth body to ensure that the body is able to effectively undertake its charter in the face of Year 2000 problems which may arise as we approach the next century and beyond. It is important to observe that the successful resolution of the Year 2000 problem will depend on the actions of each Commonwealth body.

Absolute assurances about service continuity cannot be given at this stage (Paras. 1.22 & 5.26)

8. The audit found that, in general, the eight selected bodies have established Year 2000 projects and associated governance and control structures to provide assurance to executive management about the management of Year 2000 risks. However, the ANAO cannot, at this time, offer any assurance that the selected Commonwealth bodies will become Year 2000 compliant or that they will not experience interruptions to business critical functions or services as a result of the Year 2000 problem. Nor is it possible to extrapolate from the findings for the eight selected bodies to the whole of the Australian Public Service.

Additional resources have been applied to the Year 2000 Problem (Paras. 2.29, 2.32 & 2.43)

9. Since the ANAO last reported, OGO's whole-of-government coordination role has been augmented as a result of the Government's decisions in relation to the implementation of a mandatory quarterly reporting framework and the establishment of the $120 million seed fund for approved Year 2000 activities. These initiatives, together with Commonwealth bodies' own actions, have encouraged greater executive management focus on the Year 2000 problem and have enabled the application of additional resources.

Whole-of-government reporting framework has improved management focus (Para. 2.14)

10. The quarterly reporting framework administered by OGO has served to raise awareness about, and focus ministerial and executive management attention on, the Year 2000 problem. The mandatory nature of the reporting framework has required Commonwealth agencies to self-evaluate their Year 2000 efforts and has reinforced executive management accountability for progress against the Government's prescribed milestones.

Cost estimates not supported by a comprehensive costing model (Para. 2.19)

11. The absence of a comprehensive Year 2000 costing model and the utilisation of a generic reporting framework have entailed some necessary compromises in relation to the quality and comparability of information provided by Commonwealth agencies. Nevertheless, the quarterly reporting framework has helped to ensure that Commonwealth bodies are better placed to make informed decisions about the cost of remedial action and resources which still need to be devoted to the resolution of Year 2000 issues.

Successful Year 2000 projects require strong and effective governance and control (Paras. 3.1 & 3.2)

12. The selected bodies examined for the current audit exhibit differing rates of progress. Among the more important factors which contribute to the observed progress is the degree to which the Year 2000 project is linked to key governance and control structures. Other factors include: the size and complexity of the organisation; the number and variety of business systems and inputs utilised to deliver core functions; the profile, resources and duration of the organisation's Year 2000 project; and the extent and management of major organisational change initiatives.

Commonwealth bodies demonstrated elements of better practice (Paras. 3.19, 3.24, 3.47, 3.49, 3.61-3.63 & 4.18-4.20)

13. The Year 2000 projects in the eight selected Commonwealth bodies exhibit, to varying degrees, the following elements of better practice:

✓ Year 2000 project management frameworks with strong governance structures and controls;

✓ project and risk management planning covering all business areas;

✓ business impact assessment has been carried out for most business areas;

✓ business priorities and resource requirements have been identified;

✓ mechanisms to ensure regular and effective monitoring by senior management;

✓ inventories of critical business systems and applications which are subject to ongoing verification and reconciliation;

✓ remediation is under way subject to control/quality assurance processes; and

✓ test programs have been established together with mechanisms for the certification of compliance.

Embedded systems risk assessment has been late to commence (Para. 3.50)

14. Selected Commonwealth bodies' investigations of embedded systems risks affecting buildings and facilities has begun relatively late. In those bodies occupying a large number of establishments and buildings the assessment and remediation of affected systems may not be achieved within nominated time frames. Commonwealth bodies would be well advised to assess and prioritise their approach to facilities and building systems in terms of their potential impact on business continuity, security, the value of assets, occupational health and safety and public safety.

Supply-chain risks need whole-of-government focus (Para. 2.43)

15. Commonwealth bodies need to give close attention to the continued supply of essential goods and services. Commonwealth bodies are individually responsible for managing their Year 2000 purchasing risks and ensuring business continuity in the face of potential interruptions in the supply of business critical goods and services. Nevertheless, Commonwealth bodies could benefit from the provision of practical advice about better practices utilised by public and private sector organisations to manage Year 2000 supply chain risks. The whole-of-government management of supply-chain risks would be assisted by raising industry awareness of the Commonwealth's requirements as a purchaser of a range of essential goods and services.

Risks to essential infrastructure have to be addressed (Para. 2.53)

16. The continued supply of essential infrastructure services such as telecommunications, electricity, water and sewerage is a matter of vital concern to Commonwealth bodies and the community generally. Interruptions in the supply of these services could impair the delivery of key government functions and entail significant financial and human costs. No analyses have been prepared for the Commonwealth examining the likelihood of service interruption, possible impacts or whole-of-government contingency options. OGO has had limited success in obtaining information from Australian utility suppliers and is continuing to seek clarification about utility suppliers' Year 2000 status on behalf of the Commonwealth.

Contingency planning needs to start now (Paras. 2.63 & 4.38-4.41)

17. A number of selected bodies have commenced the development of contingency, business continuity and/ or business resumption plans for the management of residual Year 2000 risk, although the nominated time frames for completion vary. There is a need for the development of whole-of-government continuity management and contingency plans in order to avoid or minimise the disruption of key Government functions and services. Such action would be in line with the Government's statements concerning the development of contingency plans to deal with potential interruptions of essential infrastructure.

Coordinated communication strategies are necessary (Para. 2.64)

18. Communication strategies will be an important element of continuity management arrangements for individual Commonwealth bodies. These may comprise messages designed to manage stakeholder perceptions of the Year 2000 risks to services as well as communication strategies for the provision of public advice or instruction in the event of any interruption of services. Communication strategies need to be coordinated at a whole-of-government level in order to reduce the potential for confusing or contradictory public messages; to avoid potential adverse effects of unintended messages; and to inform the community about the actions being taken to ensure the continuity of key government services.

Organisational change can delay preparations unless carefully managed (Paras. 5.15-5.17)

19. Each of the selected Commonwealth bodies has recently experienced, or will undergo, some degree of organisational change. Each of the selected bodies recognises the risks that Year 2000 projects may be adversely affected by competing demands on executive management attention and resource competition in a change environment. Selected bodies acknowledge the potentially heightened risk to the continuity of Year 2000 effort as a result of implementing changes to business critical systems, particularly during the latter half of 1999. Selected bodies also recognise the opportunities presented in a change environment to rationalise, renovate and/or replace business systems and, thereby, reduce their Year 2000 exposures.

Risks need to be managed into the next century (Para. 5.26)

20. Selected Commonwealth bodies have established Year 2000 project management systems and structures necessary to effectively manage their Year 2000 risks and achieve outstanding targets provided they maintain their current level of effort and there is no marked change in their operating environments. After the turn of the century, all Commonwealth bodies will have to validate the performance of critical systems as well as continue the remediation and testing of non-critical systems. However, major organisational changes and/or the implementation of new business systems to support new policy initiatives could affect the progress of Commonwealth bodies' Year 2000 projects.

Recommendations

Six recommendations agreed, or agreed with qualification for improved Year 2000 preparedness

21. The ANAO made six recommendations which were agreed, or agreed with qualification. Recommendations 1 to 3 concern the following whole-of-government issues: the management of Year 2000 risks to the supply of essential goods and services; analysis of the potential for the interruption of utility services and impacts on key government services; and aspects of the Year 2000 problem which require a whole-of-government approach to continuity management. Recommendations 4 to 6 concern the following agency/entity level responsibilities: the development of contingency plans; the incorporation of Year 2000 impact statements in proposals leading to the implementation of major organisational or business changes; and post-2000 performance of business processes to ensure correct functioning.

Recommendations

Set out below are the ANAO's recommendations. The ANAO considers that priority should be given to Recommendations 3, 4 and 5.

Recommendation No.1 Para. 2.44

ANAO recommends that the Department of Communications, Information Technology and the Arts, through the Office for Government Online:

(a) identify and encourage the application by Commonwealth bodies of better practices in relation to the effective management of Year 2000 risks to the supply of essential goods and services; and

(b) formulate strategies to raise industry awareness of the Commonwealth's requirements in relation to the management of its Year 2000 risks.

Agree: Airservices, ATO, Centrelink, Customs, Defence, DETYA, DIMA and OGO (1a).

Agree with Qualification: OGO (1b).

Recommendation No.2 Para. 2.54

ANAO recommends that the Department of Communications, Information Technology and the Arts, through the Office for Government Online:

(a) continue making direct approaches to utility suppliers and complement these actions with approaches to relevant representative industry bodies and regulatory authorities; and

(b) together with relevant lead agencies, coordinate the preparation of a risk analysis of the potential for the interruption of utility services and assess the potential impacts on key government services.

Agree: Airservices, ATO, Centrelink, Customs, Defence, DETYA, DIMA and OGO (2a).

Agree with qualification: OGO (2b).

Recommendation No.3 Para. 2.65

ANAO recommends that the Department of Communications, Information Technology and the Arts, through the Office for Government Online:

(a) convene urgent discussions with relevant Commonwealth bodies to identify and provide advice to Government on aspects of the Year 2000 problem which require a whole-of-government approach to continuity management; and

(b) consult relevant Commonwealth bodies in the development appropriate communication strategies to inform clients, stakeholders and the community generally about arrangements for continuity management in relation to key Government functions.

Agree: Airservices, ATO, Centrelink, Customs, Defence, DETYA, DIMA and OGO.

Recommendation No.4
Para. 4.42

ANAO recommends that Commonwealth bodies that have not already done so, give urgent attention to the development of contingency plans, including emergency response and resumption plans, which address Year 2000 within an overall continuity management approach.

Agree: Airservices, ATO, Centrelink, Customs, Defence, DETYA, DIMA and RBA.

Recommendation No.5
Para. 5.18

ANAO recommends that Commonwealth bodies incorporate Year 2000 impact statements within all proposals or submissions leading to the implementation of major organisational or business changes.

Agree: Airservices, ATO, Centrelink, Customs, Defence, DETYA, DIMA and RBA.

Recommendation No.6
Para. 5.27

ANAO recommends that Commonwealth bodies:

(a) comprehensively review their progress to date; assess the Year 2000 targets and milestones which must be achieved in the time remaining; and identify potential risks to the achievement of compliance for business critical systems and functions;

(b) identify activities to be undertaken to renovate, replace or retire remaining systems; guard against re-occurrence; and audit the post-2000 performance of business processes to ensure correct functioning; and

(c) prepare a Year 2000 transition plan, using a documented process for accountability and awareness-raising purposes, to manage the migration of dedicated Year 2000 resources and control structures to a 'business-as-usual' environment during the calendar Year 2000.

Agree: Airservices, ATO, Centrelink, Customs, Defence, DETYA, DIMA and RBA.

Audit Findings and Conclusions

1. Introduction

This chapter outlines the rationale, approach and methodology for the audit into Commonwealth agencies' progress with the Year 2000 problem.

Background

1.1 The Year 2000 problem refers to the inability of some computer programs and micro processors to recognise or perform calculations using either a four digit year date or a two digit year date where the year 2000 is represented as '00'. This may result in the program failing to operate correctly, either by shutting down or producing erroneous results.

1.2 The information technology (IT) industry has been aware of the Year 2000 problem since the 1970s. In the 1970s and 80s it was generally thought that technologies using two digit date fields would be retired and replaced well before the turn of the century. However, much of the IT infrastructure commissioned during the last two and a half decades has proven to have a longer working life than was originally expected. Therefore, little action was taken until recently to rectify the problem. Even recently manufactured software and hardware has been proved to be affected by the Year 2000 problem. As a result, organisations have to be concerned not only with their legacy systems, but must also carefully assess even recently acquired information technology and telecommunications products and services.

1.3 Australian Governments and industry have been generally aware of the Year 2000 problem and the business implications of any failure to achieve Year 2000 compliance since the mid 1990s. Until the mid 1990s, it appears that awareness and understanding of the Year 2000 problem was largely confined to IT professionals. However, there is a growing awareness that the Year 2000 problem is not just an IT problem and, in fact, represents potential risks to business viability.

1.4 The business processes of most public and private sector organisations utilise IT&T. Larger organisations, in particular, rely upon often complex information technology systems which can be made up of many applications, each of which is potentially affected by the Year 2000 problem. In addition, individual systems often have to interface with other systems or applications and these interfaces may be internal and/or external to the organisation. A Year 2000 failure for one application, therefore, has the potential to cause significant disruption to whole systems. In turn, Year 2000 failures can cause disruptions to an entire organisation and even to other organisations with which it has a business relationship.

1.5 The core business functions of Commonwealth bodies are increasingly reliant on IT&T. The business processes of many Commonwealth bodies have been extensively re-engineered to accommodate the introduction of new technologies. Technological adaptations have been used to capture greater efficiency, improve customer/client accessibility and responsiveness, and cope with dramatic increases in the volume of transactions. The extent of business process automation means that, in the event of any Year 2000 disruption to automated business systems, some Commonwealth bodies may not be able to substitute manual processes. In others, the substitution of manual processes may entail significant losses in productivity, efficiency and service quality. This will be particularly true of larger organisations whose business exposure to IT&T-enabled business processes is usually proportionally greater.

Audit rationale

1.6 The Year 2000 problem has presented a significant challenge to governments and industry. The size and complexity of business operations and business systems means that, for many Commonwealth bodies, rectifying the Year 2000 problem will be one of the largest IT implementation projects they have ever managed. However, studies carried out overseas and in Australia indicate that government organisations have been slow to respond to the Year 2000 problem.[1] Not only can the deadline to achieve Year 2000 compliance not be deferred, year date malfunctions have already begun to occur in cases where business systems have been required to perform operations using dates from 2000 and beyond.

1.7 The Year 2000 problem is a whole-of-business issue, not just an IT problem. This means that solutions to the Year 2000 problem require the mobilisation of people and resources across an organisation's operations. Nor is the Year 2000 problem purely internal to an organisation. Few organisations operate in isolation: this is as true for Commonwealth bodies as it is for private sector organisations. In many cases, Commonwealth bodies have had to work closely with their suppliers, customers and business partners to address aspects of the Year 2000 problem which are of common concern. For example, organisations frequently exchange data by electronic means or rely on electronic funds transmission to pay their

[1] In Australia, a report entitled *Year 2000 Survey Results* (November 1997) prepared by Coopers & Lybrand with the support of the Institute of Chartered Accountants in Australia, observed that responses to the survey indicate that *the Government sector (Commonwealth and local), is slower in reacting to Year 2000 issues, and is approximately 6 months behind the private sector* (p. 16).

employees, suppliers, contractors or beneficiaries. In addition, organisations often depend on the uninterrupted supply by third parties of goods and services, the continued production of which could be affected by a Year 2000 failure. Of particular concern to most organisations is the continued supply of telecommunications, electricity, water, gas and sewerage.[2]

1.8 For most organisations, the Year 2000 problem will not be the only business problem they are required to address between now and 2000. No organisation is immune to change or the requirement to adapt to a changing environment. Government bodies exist to implement the policy directions of Government and, by and large, do not exercise the same degree of management autonomy as private sector organisations. From the commencement to the completion of their Year 2000 project, many Commonwealth bodies have been required to simultaneously manage changes to their organisational arrangements (including re-organisations, amalgamations and the establishment of new organisations); the implementation of new programs and services (and associated business processes); and the implementation of administrative reforms mandated by Government (such as the outsourcing of IT).

1.9 Major projects of this nature are naturally resource intensive and, where they occur simultaneously, are often in competition for the same human and technical resources required by Year 2000 projects. Frequently too, projects flowing from the implementation of Government policy operate according to stringent time-tables (such as those set out in legislation). Occasionally, major change initiatives can complement and contribute to the achievement of Year 2000 objectives. Examples are IT outsourcing, which can provide strong incentives to compile, verify and assess IT inventories (an early, necessary step in any organisation's Year 2000 project); or the commissioning of business systems to support new programs and services (which may result in non-Year 2000-compliant business systems being retired and replaced).[3]

[2] Three events in 1998 - none of which was caused by the Year 2000 problem - provide a signpost to the possible effects of any widespread interruption in the supply of critical utilities. The first was the Auckland (New Zealand) blackout which saw a series of electricity supply failures affecting the Auckland central business district between February and April 1998. The blackout caused significant hardship for businesses and consumers and necessitated the implementation of disaster plans by hospitals and emergency services. The second event was the August 1998 contamination of the Sydney water supply which posed both a public health risk and imposed additional costs on the community. The third was the September 1998 interruption of gas supply in Victoria as a result of an explosion at Victoria's main gas plant. Many organisations are currently factoring potential failures in electricity, water and sewerage into their Year 2000 contingency, disaster recovery and business continuity plans.

[3] Although competing business initiatives can contribute to an organisation's Year 2000 efforts, the simultaneous management of major implementation projects nevertheless represents a potential risk to an organisation's Year 2000 project.

Previous audit coverage

1.10 In mid 1997 the ANAO surveyed a wide range of Commonwealth bodies to ascertain the appropriateness and adequacy of their approach to the identification and management of Year 2000 related risks. The audit[4] addressed selected bodies': planning in relation to achieving Year 2000 compliance; implementation, management and monitoring of Year 2000 compliance strategies; strategic risk assessments in relation to the Year 2000 changeover; and awareness of the various aspects of the Year 2000 problem.

1.11 The previous audit's main findings are summarised below:

- less than half of the bodies surveyed were able to provide estimates of the total cost for their organisation to become Year 2000 compliant, however, this could be addressed, in part, by a more systematic approach to risk management;
- most bodies needed to do much more to address their Year 2000 problem and would need to increase their Year 2000 effort and provide reliable assurances about their management of business risks associated with the Year 2000 problem;
- most bodies had not adequately analysed and established priorities for their Year 2000 risks from a whole-of-business perspective;
- many bodies had only a partial understanding or appreciation of the potential implications of the Year 2000 problem for their functions and business processes;
- although the preparation of inventories of Year 2000 affected products and services had commenced, this work was not well advanced in most cases;
- most bodies had not undertaken any compliance testing of their systems and applications and were, therefore, unable to offer assurances that their systems would operate as required in the year 2000; and
- many bodies had not: established a Year 2000 project; designated an overall Year 2000 project manager; or defined the roles and responsibilities of individuals responsible for responding to the Year 2000 problem.

1.12 The previous audit report contained eight recommendations which were agreed, or agreed with qualification by agencies.

[4] ANAO, *Managing the Year 2000 Problem - Risk Assessment and Management in Commonwealth Agencies*, Audit Report No. 27, December 1997.

Other audit reviews

1.13 Audit Offices in Australia and overseas have reported on public sector organisations' efforts to achieve Year 2000 compliance. The General Accounting Office (GAO) has been especially active and has produced a number of reports on the preparedness of Federal agencies in the United States of America.[5] In March 1998 the GAO made the following observation:

> *Despite the efforts of each business, state and local government, and federal agency to race against time and renovate, validate, and implement their mission-critical information systems every organisation remains vulnerable to the disruption of its business processes.*[6]

1.14 The United Kingdom National Audit Office (NAO) reported in May 1998 on the progress of departments and agencies based on a review of plans produced between October 1997 and February 1998, and March 1998 returns to the Central Information Technology Unit (CITU). Among the broad conclusions set out in its Report, the NAO observed the following:

> *The returns submitted to the CITU in March 1998 do not give confidence that all departments and agencies have yet identified the full extent of the millennium threat, have assessed the risks and have prioritised work to resolve the problem… The evidence from the plans and progress reports in March 1998 suggest that departments and agencies are still vulnerable to risks of failure which have not been fully assessed. Many bodies do not have contingency plans in place, and a small proportion of bodies consider such plans as unnecessary.*[7]

1.15 The Controller and Auditor-General for New Zealand reported in December 1997 that :

> *All entities were confident that they will meet their deadlines for Year 2000 compliance. However, some have yet to complete their inventories or fully examine their exposure to external parties… We are not as confident as the entities that they will meet their deadlines unless they make significant progress over the coming months.*[8]

[5] Electronic versions of GAO reports may be obtained from the GAO's World Wide Web server at the following Internet address <***http://www.gao.gov***>. GAO reports address the Year 2000 preparedness across a number of key government sectors including Defence, Social Security, Financial Regulation, Taxation and Air Safety.

[6] United States General Accounting Office, *Year 2000 Computing Crisis: Business Continuity and Contingency Planning*, Exposure Draft, March 1998, p. 2 (Source: ***http://www.gao.gov***).

[7] Report by the Comptroller and Auditor General, *Managing the Millennium Threat II*, National Audit Office, London, 15 May 1998, pp. 22-23.

[8] Report of the Controller and Auditor-General, *Is the Public Sector ready for the Year 2000?*, December 1997, p. 18.

1.16 Among the Australian State Audit Offices which have reported on the preparedness of public sector organisations are the Victorian Auditor-General's Office[9], the Tasmanian Audit Office[10], the Auditor-General's Department of South Australia[11] and the Audit Office of New South Wales[12]. The conclusion reached by the Auditor-General for Tasmania is generally representative of the broad findings in each jurisdiction:

> *Based on the evidence I collected, I conclude that while a small number of organisations are making good progress towards resolution of the Year 2000 problem, the public sector generally was not well advanced, at the time of the survey, in preparations to deal effectively with the business risks associated with the Year 2000 problem.*[13]

Audit approach

1.17 The current audit examined eight selected Commonwealth bodies' further actions to address risks associated with the Year 2000 computer problem. The broad approach to the audit is illustrated in Figure 1.1.

Objectives

1.18 The audit objectives were to assess, for selected Commonwealth bodies:

- the extent to which recommendations arising from the previous audit have been implemented;
- the extent to which Year 2000 projects demonstrate accepted elements of better practice;
- the application of appropriate financial and human resources to Year 2000 activities and the impact of Year 2000 resource deployment on non-Year 2000 IT and business initiatives;
- progress against accepted Year 2000 project milestones given selected bodies' organisational and operational profiles; and

[9] Victorian Auditor-General's Office, *Report on Ministerial Portfolios May 1998,* Part 3.7 State Development, Paras 3.7.1 to 3.7.33.

[10] Tasmanian Audit Office, Report of the Auditor-General, *The Year 2000 Are We Ready?*, Special Report No 25, March 1998.

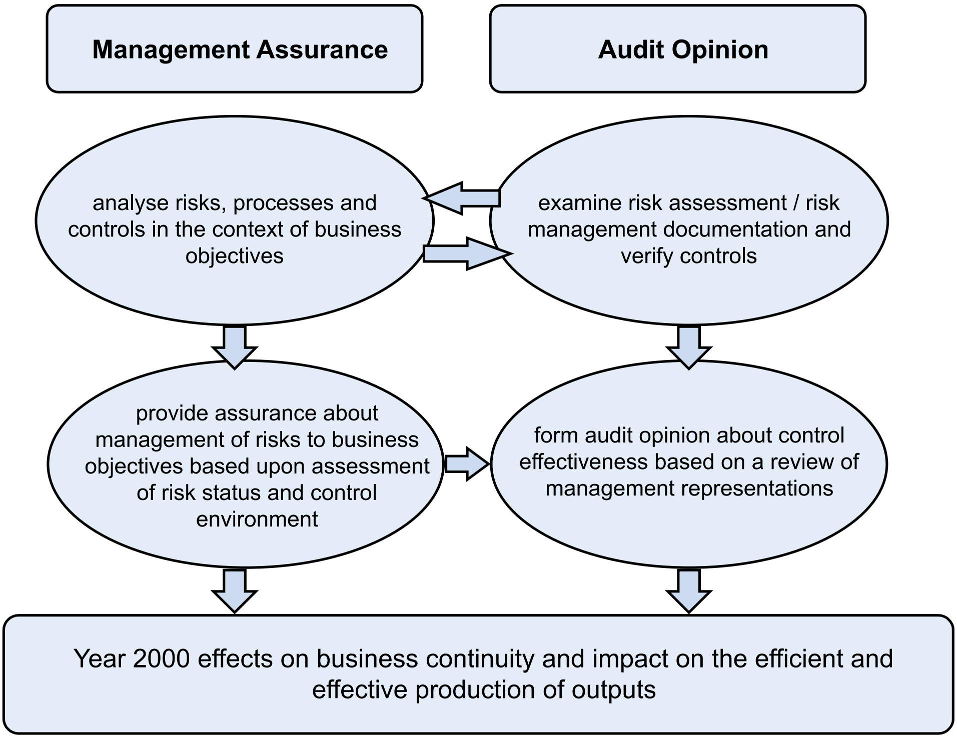
[11] Auditor-General's Department of South Australia, *Report of the Auditor-General for the Year Ended 30 June 1997*, Part A3, Audit Overview, Information technology, pp A3-88 to A3-89, December 1997.

[12] The Audit Office of New South Wales, Performance Audit Report, *1999-2000 Millennium Date Rollover - Preparedness of the NSW Public Sector*, December 1997.

[13] Report of the Auditor-General, Special Report No. 25, *The Year 2000 - Are We Ready?*, March 1998, p. 6.

- confidence levels in relation to: assessment of risks to business critical activities; implementation of risk mitigation strategies; and the likelihood of resolving Year 2000 risks to business critical functions.

Figure 1.1
Audit Approach


Management Assurance
Audit Opinion
analyse risks, processes and controls in the context of business objectives
examine risk assessment / risk management documentation and verify controls
provide assurance about management of risks to business objectives based upon assessment of risk status and control environment
form audit opinion about control effectiveness based on a review of management representations
Year 2000 effects on business continuity and impact on the efficient and effective production of outputs

Source: ANAO based on a paper presented by Bruce W. McCuaig at IIA Australia SOPAC '98, *Emerging Themes in Integrating Risk Management,* 4 March 1998.

Methodology

1.19 The ANAO undertook field work in eight selected Commonwealth bodies to ascertain their progress with the management and resolution of Year 2000 risk exposures. The ANAO field work focused primarily on Commonwealth bodies' governance of their Year 2000 efforts and the control systems established to support decision-making, coordination, acquittal and monitoring of their Year 2000 activities. The ANAO examined the extent to which selected Commonwealth bodies recognised Year 2000 issues as a potential threat to business continuity and were giving these issues priority within a coherent management and governance framework.

1.20 Field work was undertaken during the period from June to September 1998 in the following Commonwealth bodies: Airservices Australia (Airservices); Australian Customs Service (Customs); Australian

Taxation Office (ATO); Centrelink[14]; Department of Defence (Defence); the then Department of Employment, Education, Training and Youth Affairs (DEETYA, now *DETYA*)[15]; Department of Immigration and Multicultural Affairs (DIMA); and Reserve Bank of Australia (RBA). These bodies are responsible for the delivery of a range of key government functions (see Figure 1.2), including revenue collection (ATO and Customs), social welfare (Centrelink and DETYA), public safety (Airservices, Defence), national security (Defence, Customs and DIMA) and economic regulation (RBA). The ANAO also reviewed the Office for Government Online's (OGO, formerly the Office of Government Information Technology, or 'OGIT') whole-of-government coordination of the Commonwealth's Year 2000 efforts.[16] OGO's responsibilities in relation to the Year 2000 problem are described in chapter 2.

1.21 Two of the selected bodies (RBA and Airservices) are off-budget Commonwealth entities. The remaining six are budget funded Commonwealth agencies. Collectively, the six budget funded agencies account for approximately 50 per cent of total Government expenditure.[17] The ATO and Customs together account for approximately 99 per cent of contributions to Government revenue.[18] The RBA is responsible for the management of over $47 billion in assets.[19]

1.22 The audit reports on the progress of selected bodies' Year 2000 projects and assesses the integrity of the governance and control structures established to provide assurance to executive management about the management of Year 2000 risks. The ANAO cannot offer any assurance that selected bodies will become Year 2000 compliant or that they will not

[14] Until October 1998, Centrelink has managed the Year 2000 issue, on a portfolio basis, for the former portfolio of Social Security. This consisted of Centrelink, the Department of Social Security and the Social Security Appeals Tribunal. With the portfolio changes announced by the Government in October 1998, these three agencies are now parts of the new Family and Community Services Portfolio. Centrelink advised the ANAO that the details of how the Year 2000 issue will be managed in the new portfolio have not yet been determined.

[15] As a result of changes in administrative arrangements announced in October 1998, responsibility for employment services transferred to the new Department of Employment, Workplace Relations and Small Business. Although this report will refer to the Department by its new name (DETYA, unless otherwise indicated by the context) the finding contained in this report pertain to the former *DEETYA* (including the employment services component).

[16] In October 1998 the Government announced OGIT's transfer from the Finance and Administration portfolio to the Communications, Information Technology and the Arts portfolio. It was also announced that OGIT would be renamed the Office for Government Online (OGO). This report will refer to OGO unless the context of the discussion dictates otherwise, for example, where reference is made to past actions taken by the former OGIT.

[17] The Commonwealth Public Account - Budget Paper No.4 (Tables 1, 6 and Schedule to Appropriation Bill (No.1)).

[18] Ibid., Budget Paper No.4 (Tables 1 and 5).

[19] Reserve Bank of Australia 1998, Report and Financial Statements, p. 73.

experience interruptions to business critical functions or services as a result of the Year 2000 problem. Nor is it possible to extrapolate from the findings for the eight selected bodies to the whole of the Australian Public Service.

1.23 In the course of this audit the ANAO utilised the following consultants: (the then) Coopers & Lybrand to assist with the development of audit criteria; Mr Jim Humphreys, who reviewed initial drafts of the ANAO's analysis; and KPMG Management Consultants, to facilitate a workshop on issues arising from the audit involving selected Commonwealth bodies and OGO. The cost of the audit was approximately $237 000. The audit was conducted in accordance with the ANAO Auditing Standards.

Report Outline

1.24 Chapter 2 examines OGO's whole-of-government management of the Year 2000 problem on behalf of the Commonwealth. Chapter 3 examines the extent to which selected Commonwealth bodies have established core planning and project management elements; compiled inventories of affected systems; and assessed likely impacts and are appropriately managing their Year 2000 resource requirements. Chapter 4 examines selected Commonwealth bodies' progress with the remediation and testing of Year 2000 affected systems and the establishment of mechanisms for quality assurance, certification of compliance and contingency planning. The final chapter examines selected Commonwealth bodies' management of Year 2000 project risks associated with organisational change processes and considers what selected Commonwealth bodies need to achieve between now and 2000.

Figure 1.2
Profile of Commonwealth Bodies Selected for this Audit

Background

The bodies selected for review in the current audit are responsible for the administration of important Government programs and the delivery of essential Government services. Their business processes are extensively automated and highly reliant on information technology. Each is also reliant on a range of business partners, suppliers and essential infrastructure services. Therefore, the Year 2000 problem poses a potential threat to the continued delivery of their services.

Airservices Australia (Airservices) is a wholly Commonwealth owned commercial entity providing airspace management, air traffic control, traffic and flight information, navigation services, aeronautical information and fire fighting services within Australia's sovereign airspace and in international airspace over the Pacific and Indian Oceans.

Australian Customs Service (Customs) is the second largest revenue collection agency after the ATO and performs other key functions in relation to the facilitation of trade and compliance, travel facilitation and compliance, the delivery of industry support and coastal and offshore surveillance and response.

Australian Taxation Office (ATO) is responsible for the collection of taxation revenue and exercises functions in relation to child support and retirement income. Business disruption could affect the receipt and processing of Commonwealth revenue and adversely affect taxpayers.

Centrelink is responsible for the delivery of a range of Commonwealth social welfare payments (Centrelink makes around 159 million payments each year) and services, principally on behalf of the Department of Social Security. Business disruption could adversely affect Centrelink's estimated 7.8 million customers.

Department of Defence (Defence) is responsible for the defence of Australia, the promotion of regional security and response to civil emergencies. Defence's logistic capability is reliant upon a wide range of information technology inputs, including warfare assets such as warships, aircraft and landcraft equipped with high technology weapons, navigation and communications systems.

Department of Employment, Education, Training and Youth Affairs (now *DETYA*)[20] is responsible for administration of programs in the areas of education and training. Although revised administrative arrangements announced in October 1998 have resulted in the transfer of responsibility for employment services to the new portfolio of Employment, Workplace Relations and Small Business, until October 1998, Year 2000 risks to associated business systems have been managed within DEETYA.

Department of Immigration and Multicultural Affairs (DIMA) is responsible for managing the movement of people into and out of Australia. In conjunction with the Australian Customs Service, DIMA works to ensure the efficient entry and exit of genuine travellers and the detection of persons of concern and is therefore an important element in the maintenance of effective border integrity.

Reserve Bank of Australia (RBA) is responsible for the conduct of monetary policy, the main instruments of which are domestic market operations and foreign exchange operations. The RBA shares policy responsibility for the stability of the Australian financial system with the newly established Australian Prudential Regulation Authority (APRA). The RBA is closely involved in the operation of the payments and settlement systems and provides selected banking services to Commonwealth and State Government customers and some overseas official institutions.

Source: ANAO based on selected bodies' Annual Reports.

[20] See footnote No. 15.

2. Whole of Government Year 2000 Coordination

The purpose of this chapter is to review the management of the Year 2000 problem on behalf of the Commonwealth Government.

Background

2.1 The Office for Government Online (OGO) is responsible for reporting and encouraging progress towards Year 2000 compliance at a whole-of-government level and, commencing in the first half of 1996, has undertaken a central coordinating and advisory role for Year 2000 issues affecting Commonwealth bodies. This role was strengthened in September 1997, through the creation of a Year 2000 Project Office and the implementation of a mandatory quarterly reporting framework for all budget funded Commonwealth agencies. In July 1998, mandatory quarterly reporting was further extended to include off-budget Commonwealth commercial entities.

2.2 In Audit Report No. 27, 1997-98, *Managing the Year 2000 Problem: Risk Assessment and Management in Commonwealth Agencies*, the ANAO recommended that the then OGIT prepare a strategic plan to underpin its Year 2000 activities on a whole-of-government basis and that the plan should include a full risk analysis, key objectives and milestones, performance measures and desired outcomes.[21] OGIT agreed with the recommendation and subsequently developed a high level strategic plan containing fourteen key objectives for which associated risks, outcomes, milestones, performances measures, current status and costs have been identified. The plan is regularly reviewed and updated as required.

2.3 With regard to the Year 2000 problem, OGO's role is to ensure that Commonwealth bodies are aware of the potential impact of the Year 2000 problem and to encourage progress towards achieving Year 2000 compliance by July 1999.[22] To fulfil this role, OGO's Year 2000 Project Office undertakes a range of activities in four key areas:

[21] Op. cit., ANAO, Recommendation No.1, p. 16.

[22] Source: OGO Year 2000 Website - http\\www.ogit.gov.au.

- monitoring and reporting Commonwealth bodies' progress towards Year 2000 compliance;
- administering the provision of financial assistance to Commonwealth bodies to assist aspects of their Year 2000 projects;
- managing risks to the Commonwealth and continuance of Commonwealth Government functions; and
- disseminating information to Commonwealth bodies about Year 2000 management issues.

2.4 As a result of administrative arrangements announced by the Government in October 1998, OGO has assumed responsibility for the National Strategy industry program established in 1997 to identify Year 2000 issues of common interest to the Commonwealth and business.[23] The National Strategy industry program is described in Figure 2.1.

2.5 OGO has identified a number of priority issues to be pursued between now and 2000, including: contingency planning[24]; legal issues; testing strategies; and risk management. OGO's activities will continue beyond the turn of the century in order to address post-2000 issues such as the remediation of non-critical business systems and legal matters. OGO will continue to report on a quarterly basis to the Government on Commonwealth bodies' Year 2000 remediation activities through 1999 until June 2000.

Monitoring and Reporting Year 2000 Progress

2.6 The two principal mechanisms utilised by OGO for the purpose of monitoring and reporting Commonwealth bodies' progress towards Year 2000 compliance are mandatory quarterly reporting and third party reviews.

Quarterly Reporting

2.7 The requirement for all budget-funded Commonwealth bodies to report quarterly through OGO (previously, through OGIT) to the Government on their remediation status and Year 2000 readiness was announced in September 1997. The administration of the quarterly reporting framework and the preparation of consolidated quarterly reports to the Government is one of OGO's key roles.

[23] Prior to October 1998, the National Strategy industry program was located in the former Department of Industry Science and Tourism (now the Department of Industry Science and Resources).

[24] Working in conjunction with Emergency Management Australia and 'lead agencies'.

Figure 2.1:
National Strategy Industry Program

Inception

In September 1997 the Commonwealth announced the implementation of a 'National Strategy' to increase business and community awareness of the Year 2000 computer date problem.[25] The Strategy is a joint effort between all levels of government and industry. A Year 2000 National Strategy Steering Committee has been formed to develop the strategy, provide high level advice, and take a lead role in coordinating Commonwealth, State and industry initiatives to raise business awareness and understanding of the Year 2000 issue.

Organisation

The Steering Committee is chaired by the Chairman of the Australian Stock Exchange and is made up of representatives of Commonwealth, State and Territory and Local Governments, peak industry associations (Australian Chamber of Commerce, Business Council of Australia, Australian Information Industries Association) and consumer groups. The Committee has engaged a CEO and small project team to develop and implement the Strategy. The Committee also works with the Online Government Council.[26]

A marketing sub-group has been formed to coordinate State/Territory and national marketing efforts. Benefits have been realised from the exchange of information and experiences which has enabled a number of jurisdictions to fast-track their own programs. An industry council, comprising representatives of business associations, has also been established to input to the Strategy, to report on the state of preparedness of key industries, and to facilitate the development and implementation of industry specific measures.

Aims

The main aim of the National Strategy is to raise understanding by business, especially by small and medium sized enterprises, of the Year 2000 computer issue and in doing so, encourage business to undertake the necessary risk management analysis, remediation, and contingency planning action. The Strategy complements and supplements existing State Government and industry business awareness initiatives. More generally, it aims to give the Year 2000 issue a higher profile in the media and the minds of business, and the community. Australian business is being encouraged to take advantage of the opportunities that will arise from being Year 2000 ready. The National Strategy will also provide the Commonwealth Government with regular status reports and recommend national action where appropriate.

Approach

The National Strategy has adopted a phased, multi-faceted approach involving a diverse range of activities at national, state and regional levels. A major element of the awareness strategy was a national television and media advertising campaign that was launched in early July 1998. A national inquiry telephone hotline which links to response centres in the States and Territories commenced in late May 1998. Information is also being disseminated through brochures, seminars, various media outlets and on the Internet.

Source: ANAO based on information provided by DISR.

[25] The Government announced the Year 2000 National Strategy in a Joint Media Release from the Minister for Finance, the Minister for Science and Tourism. *National Strategy for 'Year 2000' Computer Bug*, 12 September 1997.

[26] A committee of Communication Ministers from each Government jurisdiction.

2.8 Through the quarterly reporting framework budget-funded Commonwealth agencies are required to provide information about their progress with the following activities: scoping and planning; conversion or upgrade; testing; implementation; and executive management sign-off. The data submitted by Commonwealth agencies through the quarterly reporting framework enables OGO to provide aggregate reports to the Government[27] concerning:

- the number of business critical systems in each agency;
- the rate of progress towards compliance in accordance with better practice targets for the principal phases of activity;
- an assessment of the potential risk that compliance may not be achieved based on the Year 2000 compliance target dates nominated by agencies; and
- indicative Year 2000 costs, including costs to date and estimated costs for the completion of Year 2000 work.

2.9 The first quarterly report was provided to Ministers in December 1997 with subsequent reports in February 1998 and May 1998. For the third quarter of 1998, the normal reporting procedure was varied for the caretaker period leading up to the 3 October general election, and a brief was provided to the Minister for Finance and Administration. In July 1998, the Government issued the first of a series of public updates on the work being done on the Commonwealth's own systems.[28] Also in July 1998, the Minister for Finance and Administration announced that the quarterly reporting framework was to be extended to include Commonwealth owned commercial (off-budget) entities. This class of entities comprises Government Business Enterprises, Public Trading Enterprises, Public Financial Enterprises and Statutory Marketing Authorities.[29]

2.10 Commercial entities are required to report, in broad terms, the percentage of IT and non-IT systems subject to the four phases of the compliance process: scoping and planning; remediation; testing; and,

[27] OGO has informed the ANAO that the Department of Defence reports on a different basis to the rest of the Commonwealth. By agreement with OGO, Defence's Year 2000 progress is reported in terms of business critical *functions* rather than business critical *systems*. As a result, OGO's assessment of Defence's progress is reported separately to other Commonwealth agencies and data provided by Defence are not included in OGO's whole-of-government assessments.

[28] Minister for Finance and Administration, *Commonwealth Year 2000 (Y2K) Progress Report*, Media Release 63/98, 7 July 1998. The update provided summary data for five groups of critical services: health and national safety; payments, social welfare and employment; revenue collection; national security; and defence.

[29] In addition, the Treasurer; the Minister for Communications, Information Technology and the Arts; and the Minister for Transport and Regional Services will report on the status of Year 2000 activities/readiness on a whole of sector basis in the banking and financial services, communications, and airports and air traffic control sectors respectively.

implementation/compliance. Entities are also required to provide estimated costs of Year 2000 remediation for the 1997-98, 1998-99 and 1999-2000 financial years. OGO reports that the majority of entities (96 per cent)[30] have reported and results will be included in the fourth quarterly report for 1998. A decision has not yet been taken about whether the compliance status of Commonwealth commercial entities will be publicly reported.

2.11 OGO's Year 2000 Project Office monitors the quality of quarterly reports and works with bodies to encourage compliance with the reporting requirement.[31] OGO reports that Commonwealth agencies' compliance with the reporting requirement has improved since the introduction of the reporting framework. Whereas only 84 per cent of budget-funded agencies (105 out of, then, 125 agencies) reported for the first quarter of 1998, OGO now advises that compliance has improved in each subsequent quarter and that 100 per cent (127 out of a current 127 agencies) submitted reports in the fourth quarter of 1998. Relevant Ministers and Chief Executives are provided with an individual assessment of each body's progress in relation to the Commonwealth's Year 2000 milestones.

2.12 In September 1998, the ANAO convened a focus group involving a number of larger Commonwealth agencies for the purpose of discussing whole-of-government Year 2000 coordination activities.[32] The participating agencies suggested that, for a number of reasons, the information provided through the quarterly reporting framework may not accurately represent individual agencies', or the Commonwealth's aggregate position.[33] OGO reports that a number of, particularly smaller, agencies have adopted the quarterly reporting framework as a management tool for their Year 2000 projects. A number of larger agencies, however, report using internally designed reporting mechanisms which better reflect their operating environment. In such cases, the transfer of data from Commonwealth

[30] OGO reported that it was in the process of clarifying the status of two Government entities which have not responded to the request for a report on compliance.

[31] To reinforce the urgency of the Year 2000 problem the Minister for Finance and Administration wrote to Ministers on 15 January 1998. The Year 2000 problem was discussed at the Portfolio Secretaries' meeting of 4 March 1998 and correspondence from The Chief Government Information Officer (CGIO) to agency heads followed on 7 April 1998.

[32] The focus group was held on 2 September 1998, and involved Year 2000 coordinators from the then DEETYA, Customs, ATO and Centrelink. These bodies deliver a number of key government functions and represent a significant proportion of Commonwealth expenditure and revenue. The focus group addressed a number of key issues. References to 'larger agencies' views in this chapter refer to the views of the four agencies participating in that workshop. It should be noted that the views expressed by representatives of the four agencies are not necessarily representative of all (and in particular, small) Commonwealth bodies.

[33] The larger agencies participating in the September focus group commented that the reporting framework is built upon a number of assumptions which are not directly applicable to their business context; some of the terms and definitions are loosely applied; and agencies do not necessarily report on a consistent or comparable basis.

agencies' Year 2000 project data bases into the quarterly reporting framework can result in a consequential loss of detail or accuracy.[34]

2.13 The quarterly reporting requirement has served to capture the attention of decision-makers and to reinforce the importance of the Year 2000 problem as a business continuity issue requiring timely action and effective risk management. Agencies generally agree that quarterly reporting has provided a useful focus on the Year 2000 issue at a whole-of-government level and that further refinement of the quarterly reporting framework at this time would be unproductive.

2.14 **Finding:** The quarterly reporting framework administered by the Office for Government Online has served to raise awareness about, and focus ministerial and executive management attention on the Year 2000 problem. The mandatory nature of the reporting framework has required Commonwealth agencies to self-evaluate their Year 2000 efforts and has reinforced executive management accountability for progress against the Government's milestones.

Costing Year 2000 Activity

2.15 The quarterly reporting framework requires Commonwealth agencies to estimate their Year 2000 costs for each financial year until June 2000. Agencies' estimates are used as a basis for calculating the possible aggregate Year 2000 costs for all Commonwealth agencies. In its previous report the ANAO found that that less than half of the bodies surveyed were able to provide estimates of the total cost for their organisation to become Year 2000 compliant.[35] The audit revealed that Commonwealth bodies did not have access to a consistent and systematic methodology for the analysis and projection of Year 2000 costs. The ANAO recommended that the then OGIT, in consultation with lead agencies, develop a costing model to be used by Commonwealth bodies to reliably and accurately estimate their Year 2000 costs.[36] At that time, OGIT responded that the

[34] The larger agencies participating in the September focus group consider that the quarterly reporting framework *under*-represents their progress by constraining the provision of Year 2000 project information within inflexible categories. These agencies acknowledge that adjustments were made to the framework in accordance with agencies' representations and consider that further adjustment to the framework will not result in significant improvement.

[35] Op. cit., ANAO, p. 19.

[36] Ibid, Recommendation No.2, p. 19.

quarterly reporting framework then being developed would bring about more consistent cost estimates.[37]

2.16 The eight selected Commonwealth bodies reviewed for the current audit reported an estimated total cost to achieve Year 2000 compliance of $293.4 million. The six budget-funded Commonwealth agencies reported total estimated Year 2000 costs of $286.3 million, of which approximately two thirds is accounted for by the Department of Defence.

2.17 The Chief Government Information Officer (CGIO) noted in correspondence to Chief Executives in July 1998 that not all agencies had identified their costs in addressing the Year 2000 problem. It was also noted that some Commonwealth bodies have requested advice about a costing model to use in relation to their Year 2000 projects and suggested that bodies refer to the publication *Value for your IT dollar—Guidelines for Cost-Benefit Analysis of Information Technology Proposals*.[38] This is additional to the general guidance provided to Commonwealth bodies for the purposes of completing their quarterly returns.

2.18 The extent to which the *Guidelines for Cost-Benefit Analysis of Information Technology Proposals* has been used by Commonwealth bodies as an aid in the estimation of Year 2000 costs is not known. Although these Guidelines provide a useful starting point, particularly in relation to the IT component of an organisation's Year 2000 costs, it is not clear that they provide a sufficient basis for the estimation of the full range of direct and indirect costs to address Commonwealth bodies' Year 2000 problem. Larger agencies report that direct Year 2000 costs are difficult to separate from other forms of IT expenditure and observe that, in many cases, reported expenditure may be significantly under-estimated or over-estimated. Accordingly, reported expenditures and estimates have not been prepared on a consistent basis and are not necessarily comparable between agencies.

[37] The then OGIT agreed with qualification to the recommendation, and advised that: *since the ANAO survey, OGIT has established a Year 2000 Reporting framework for agencies to report on a number of elements of their Year 2000 activities, including the estimated costs of addressing the Year 2000 issue. Agencies have been asked to provide costing information for the fiscal years ending 1997, 1998, 1999 and 2000 on the following categories: Year 2000 costs of non IT and IT business critical systems; Year 2000 project management costs; Year 2000 integration testing costs; Year 2000 costs for non-business critical systems; total Year 2000 costs; total application & maintenance budget (includes Year 2000 budget); [and] total IT budget. OGIT has also instructed agencies to restrict the estimated Y2K costs to those expenditures that are directly attributable to addressing the Year 2000 issue. OGIT is of the view that the reporting framework will bring about more consistent Year 2000 cost estimates across Commonwealth agencies.*

[38] Department of Finance, *Value for your IT dollar - Guidelines for Cost-Benefit Analysis of Information Technology Proposals, Guidelines for Cost-Benefit Analysis of Information Technology Proposals*, Canberra 1993.

2.19 Finding: The Office for Government Online has not developed a costing model to provide a consistent basis for the estimation of Commonwealth agencies' Year 2000 costs. The ANAO considers that the quarterly reporting framework, coupled with reference to the *Guidelines for Cost-Benefit Analysis of Information Technology Proposals*, do not on their own represent a sufficient response to the recommendation from the previous audit. The absence of a comprehensive Year 2000 costing model and the utilisation of a generic reporting framework have entailed some necessary compromises in relation to the quality and comparability of information provided by Commonwealth agencies. Nevertheless, the ANAO considers that the quarterly reporting framework has helped to ensure that Commonwealth bodies are better placed to make informed decisions about the cost of remedial action and resources which still need to be devoted to the resolution of Year 2000 issues.

Third Party Review

2.20 OGO has the capability to commission independent Year 2000 compliance audits of Commonwealth agencies.[39] OGO's ability to initiate third party reviews of Commonwealth agencies was increased through the application of additional resources in September 1997 and April 1998. In April 1998 the then OGIT established a panel of consultants to carry out independent reviews of up to ten agencies over the ensuing six months. The terms of the contract were to carry out reviews to determine (as a minimum):

- whether a compliance plan is in place and the extent of progress against the prescribed timetable;
- whether a full risk assessment has been developed and compliance plans formulated; and
- options for progressing Year 2000 compliance work to meet the Government's prescribed time-table.

2.21 In August 1998 the CGIO wrote to the Chief Executives of ten Commonwealth agencies representing a cross-section of key Government

[39] In May 1997 the then OGIT commissioned Coopers & Lybrand to carry out 'desk' audits of Year 2000 compliance plans in the following 13 Commonwealth agencies: Department of Social Security; (the then) Department of Employment, Education, Training and Youth Affairs; Australian Taxation Office; Australian Customs Service; Australian Bureau of Statistics; Comsuper; Department of Immigration and Multicultural Affairs; Department of Defence; (the then) Department of Finance; (the then) Department of Administrative Services; Department of Veteran's Affairs; Australian Industrial Property Organisation; and Parliamentary Information Systems Office. The results of the desk audits were directly communicated to the participating agencies in July 1997 together with recommendations.

functions[40] to request their participation in third party reviews of Year 2000 compliance.[41] Agencies were advised that the reviews would *provide Government with an additional level of assurance about delivery of its key services beyond Year 2000* and would also provide an independent assessment of their progress. Agencies were invited to share 50 per cent of the cost for each review.[42] As at mid-September 1998, reviews had been carried out in three agencies, one was under way and four had indicated a willingness to participate. Two agencies requested clarification about the purpose of the reviews on the grounds that they had been subject to external audit by the ANAO (in the context of this report).

2.22 In September 1998 the then OGIT issued a further request for tender for consultancy services to conduct third party reviews of selected budget-funded agencies over the ensuing eighteen months. Among the matters which might be considered as part of a third party review are:

- progress with meeting the Government's prescribed timetable;
- the suitability of the Year 2000 compliance plan;
- the applicability of the contingency plan;
- the accuracy of costing information;
- the depth and appropriateness of testing program(s) and test results;
- progress in meeting milestones identified in seed funding applications;
- the extent to which a risk assessment methodology has been developed; and
- options for progressing Year 2000 compliance work to meet the Government's prescribed timetable (if necessary).

2.23 Unlike the initial consultancy, there will be an increased capacity to tailor the reviews to focus on specific aspects of a body's Year 2000 project (the contract does not provide for the performance by the contractor of remediation services). OGO expects that approximately 30 reviews will be performed under contracts arising from this tender.

[40] OGO has identified 50 budget-funded Commonwealth agencies as providers of key Government services in the areas of health and national safety; revenue collection; defence; national security; and payments, social welfare and employment.

[41] OGO reports that, in addition to the invitation extended to agencies providing critical government functions, consideration will be given to agencies initiating a request for review as well as agencies considered by OGO to be 'at risk' of not meeting prescribed milestones.

[42] The indicative costs suggested for the reviews are: $5000 for agencies with 200 or fewer employees; $10 000 for agencies with between 201 and 1000 employees; $12 500 for agencies with between 1001 and 5000 employees; and $15 000 for agencies with 5001 or more employees.

2.24 Although OGO has been authorised by the Government to initiate reviews compulsorily in certain circumstances, OGO recognises the importance of gaining agencies' cooperation with the review process. OGO has also advised the ANAO that it intends to take into account the outcomes of any current or past external or internal audit or other review when making decisions about the scope of third party reviews in order to ensure that such reviews add value to participating agencies' Year 2000 projects.

2.25 **Finding:** The ANAO considers that the Office for Government Online's use of third party reviews to assess Commonwealth agencies' progress in relation to nominated Commonwealth targets is appropriate and offers the potential to add value to Commonwealth agencies' Year 2000 projects.

Financial assistance to Commonwealth agencies

2.26 The Government estimates that it will spend around $600 million on repairing the Year 2000 problem within Commonwealth budget funded agencies.[43] Whilst agencies are required to meet the bulk of their remediation costs from within existing budgets, $120 million was appropriated in the 1998-99 Commonwealth Budget for use as a 'seed fund' to encourage and accelerate existing remediation efforts in agencies responsible for the delivery of key Government functions.[44] Budget dependent Commonwealth agencies were invited to apply to OGO (previously, to OGIT) in the first of two rounds of funding.[45] Decisions on the amount of funding to be made available in the first round were at the discretion of the Minister of Finance and Administration, in consultation with the Treasurer and the relevant portfolio Minister. As a result of changes in administrative arrangements, decisions in relation to the second round of seed funding will be made by the Minister for Communications, Information Technology and the Arts in consultation with the Treasurer and the relevant portfolio Minister.

2.27 The establishment of the seed fund was announced on 15 April 1998, and the CGIO wrote to Chief Executives on 28 April 1998 to seek

[43] Minister for Finance and Administration, Media Release, *Commonwealth Year 2000 (Y2K) Progress Report* (63/98) 20 July 1998.

[44] Joint Media Release, Minister for Finance and Administration and Minister for Industry Science and Tourism, *$127 Million for Year 2000 Computer Date Problem*, (36/98) 15 April 1998. In addition to the $120 million allocated for the seed fund, $2.42 million was approved for use by the then OGIT to directly carry out a range of activities on behalf of the Commonwealth and $4.35 million was approved to augment the original $5.43 million allocated to the then DIST (September 1997) for the Year 2000 National Strategy.

[45] Year 2000 seed funds are available only to budget funded *agencies* and are not available to off-budget commercial *entities*. In this report, unless otherwise indicated, the term Commonwealth *bodies* is used to refer collectively to agencies *and* entities.

advice about Commonwealth agencies' intentions to apply for seed funding and indicative bids. Commonwealth agencies were formally advised about the eligibility criteria for funding on 1 July 1998. Applications for the first round of seed funds closed on 31 July 1998 and were assessed against the following criteria:

- agencies must demonstrate that funds sought are committed to specific and approved Year 2000 activities that will deliver key Government services, and that they will be used for no other purpose;
- agencies must provide evidence that the full range of options under running costs (carryovers, borrowings and revenue retention) have already been explored to the maximum extent possible (including resource agreements over and beyond the forward estimates period);
- the agency has been reporting quarterly on its Year 2000 progress and compliance; and
- the agency agrees to continue to disclose its progress in achieving Year 2000 compliance in its Quarterly Report.

2.28 Thirty-seven agencies applied for a total of $177 million in seed funding. Of the $120 million available as of 31 July 1998, approximately $80 million was distributed amongst the 37 agencies which applied for funds. On average, agencies received 50 per cent of their request (the range varied between 29 per cent and 100 per cent of funds requested). The six budget-funded Commonwealth agencies reviewed in the current audit reported that they had applied for a total of $105.7 million from the seed fund and that they received $41 million (about 39 per cent of funds requested).[46]

2.29 Each agency was advised of the outcome on 7 September 1998 and provided with an explanation of the assessment process, including reasons for any reduction in the amount requested. Agencies were informed that sufficient monies would be retained in the fund to allow a second round of applications in October 1998, with preference given to agencies which were unable to meet the deadline for the first round.

2.30 Funds will be allocated on a reimbursement basis. Agencies will be eligible to receive 'progress payments' for the demonstrated achievement of milestones leading to the completion of approved activities. Although the Government's decision provided that funds would be available to reimburse expenditure in the financial years 1997-98 and 1998-99, OGO has advised that activities undertaken prior to 1 July 1998 will not be eligible

[46] The RBA and Airservices, being off-budget Commonwealth entities, were not eligible to apply for seed funding.

in most circumstances.[47] In addition, OGO may, in some cases, commission third party reviews, prior to the disbursement of funds, to verify agencies' claims concerning the achievement of milestones.

2.31 **Finding:** The Office for Government Online has approved approximately $80 million (out of $120 million available) in seed funds to 37 Commonwealth budget funded agencies. OGO's approach to the disbursement of seed funds involves the approval of progress payments on the basis of the demonstrated achievement by Commonwealth agencies of milestones which culminate in the completion of approved activities.

Managing risks to the Commonwealth

2.32 OGO contributes to the management of common Year 2000 risks to the continuity of Commonwealth functions in a number of ways, including coordination activities and the provision of advice on specific areas of Year 2000 risk exposure such as purchasing and dependence on public utilities.

Coordination and information dissemination

2.33 The Year 2000 Project Office provides coordination functions and secretariat support to: the Commonwealth/State Liaison Group[48]; the Commonwealth Quarterly Forum[49]; the Year 2000 Sub-Committee[50]; and, since October 1998, the Year 2000 National Strategy Steering Committee. In addition, OGO also contributes to a range of initiatives designed to achieve a national approach to the Year 2000 problem.[51]

2.34 OGO exercises its coordination role primarily through its administration of the quarterly reporting framework and the seed fund. OGO also utilises a 'lead agency' approach whereby it facilitates the exchange of information between Commonwealth bodies and encourages the adoption of better practices.

[47] The exception being where agencies had committed funds prior to 1 July 1998 with payment to be made in 1998-99.

[48] The Commonwealth-State liaison group was established in February 1997 to address issues of mutual concern to Australian governments and comprises representatives from each State and Territory and the Commonwealth.

[49] Through the Commonwealth Quarterly Forum, initiated in November 1996, OGO briefs Commonwealth bodies about its Year 2000 activities and provides an opportunity to discuss issues of common concern.

[50] The Sub-Committee was established to support the Year 2000 Office in the coordination of its activities. The Sub-Committee is chaired by a Second Commissioner from the Australian Taxation Office, and is attended by representatives of the Departments of Defence; Education, Training and Youth Affairs; Health and Family Services and OGO. The ANAO attends as an observer.

[51] OGO is working to involve States and Territories in the coordination of a national approach to the continuity of emergency services and has advised the National Office of Local Government on approaches to ascertain the preparedness of Local Governments.

2.35 OGO carries out a wide range of communication activities[52] including the dissemination of information on diverse subjects such as risk management, legal risks[53], embedded systems, testing strategies and contingency planning.[54] OGO has appointed a Year 2000 marketing manager to oversee the coordination of information activities and the publication of Year 2000 information in both hard copy and electronic formats.

2.36 In mid 1998, the former OGIT commissioned the preparation of a comprehensive treatment of legal issues of concern to Commonwealth bodies, including advice in relation to the liability of the Commonwealth and its officers; standard certification of Year 2000 Compliance for the Commonwealth; third party liability of service providers under Commonwealth contracts; the legal implications of making public information about Commonwealth bodies' compliance; and the liability of government officials specifically engaged to work on the Year 2000 problem.[55]

2.37 Selected bodies acknowledge a need for both general and specialist information. It is likely that smaller bodies with less advanced projects and/or less means to identify and obtain information gain significant benefit from OGO's communication activities. Conversely, larger bodies report that their reliance on OGO for information is diminishing as their own information gathering efforts gain momentum. This may contribute to OGO's overall communication effort by providing a larger base of relevant information for dissemination to the broader Australian Public Service. It should be noted that it would be difficult, in practical terms, for OGO to directly meet the information requirements of every Commonwealth body.

[52] In mid-1997 the then OGIT engaged Coopers & Lybrand to prepare a Year 2000 Communications Strategy, elements of which appear to have been implemented. OGO has developed a revised Year 2000 Communications Strategy which, when approved, will be published on its web-site.

[53] OGIT previously obtained advice from the Australian Government Solicitor in relation to legal liability implications of the Year 2000 problem for the Commonwealth. This advice formed the basis of a seminar for Commonwealth bodies delivered in November 1997 and a copy of the advice was subsequently made available to Commonwealth bodies on the restricted area of OGO's Year 2000 website. Separately, the Government Law Group (Australian Government Solicitor) has delivered presentations on the legal dimension of the Year 2000 problem as a part of its continuing legal education program, and has addressed the issue in a Legal Briefing (No. 41, 27 April 1998) and the publication of a *Year 2000 Legal Issues Checklist*.

[54] Nine workshops were conducted between October 1997 and September 1998 on subjects such as testing strategies, legal issues, embedded systems, risk management, systems testing, non-IT systems testing, small agencies issues, utilities and contingency planning.

[55] The advice, entitled, *Year 2000 Legal Position of the Commonwealth of Australia* (August 1998) was prepared by Freehill Hollingdale & Page and has been placed on the restricted area of OGO's Year 2000 website where it may be accessed by authorised Commonwealth bodies.

2.38 Finding: The Office for Government Online has been effective in disseminating a range of information via a variety of media to a large number of Commonwealth bodies although the impact and relevance of this information varies between Commonwealth bodies.

Purchasing

2.39 In its previous audit the ANAO observed that greater attention needed to be given to the management of Year 2000 risks associated with the procurement of non-IT goods and services.[56] The ANAO expressed the view that bodies needed to minimise their risks through cost-effective procurement or contractual arrangements and concluded that this was an aspect of Year 2000 risk management which could benefit from guidance provided by relevant agencies such as the then OGIT. The ANAO recommended that OGIT, in consultation with the Department of Finance and Administration (DoFA), develop and promulgate guidelines to assist agencies with the management of Year 2000 purchasing risks arising from both common-use and unique supplier arrangements for IT and non-IT goods and services.[57]

2.40 OGIT agreed to the recommendation and advised that, in conjunction with the Competitive Tendering and Contracting Group in DoFA, it was working on the development of Year 2000 guidelines to assist all agencies in the management of Commonwealth contracts.[58] OGIT subsequently coordinated the development and promulgation of Year 2000 clauses in common-use and *non*-common-use contracts used by Commonwealth bodies and worked with the Office of Asset Sales and Information Technology Outsourcing (OASITO) to align Year 2000 policy with initiatives in IT outsourcing.

2.41 To assist Commonwealth bodies with their management of purchasing risk, the then OGIT made available samples of vendor letters and checklists developed by the Queensland Department of Primary Industry. Currently, OGO is compiling a register of commonly used systems and applications in order to assist the informal exchange of knowledge and information between Commonwealth bodies. Commonwealth Procurement Guidelines, issued in March 1998, instruct Commonwealth bodies to ensure that *they purchase equipment that is Year 2000-compliant*[59]. The Guidelines do not, however, provide guidance on the steps bodies

[56] ANAO, op. cit, pp. 20-21.

[57] Ibid, Recommendation No. 3, p. 23.

[58] Op. cit., ANAO, p. 23.

[59] *Commonwealth Procurement Guidelines: Core Policies and Principles*, Department of Finance and Administration, March 1998.

might take to ascertain compliance or the kinds of goods and services which might be affected. Although individually and collectively, these activities represent important and valuable contributions to Commonwealth bodies' management of purchasing risks, they fall short of what was envisioned in the ANAO recommendation previously agreed by OGIT.

2.42 **Finding:** Commonwealth bodies need to give close attention to the continued supply of essential goods and services. Although not all essential goods and services utilised by Commonwealth bodies have IT components, their manufacturing and distribution processes may be dependent on IT supported processes. The goods and services used by Commonwealth bodies could include consumables such as spare parts or other essential goods and a wide range of services, including labour. Because the Year 2000 problem can directly affect the viability of suppliers and manufacturers, Commonwealth bodies need to ascertain the actions taken by their key suppliers to address their own Year 2000 problem and, where necessary, identify alternative sources of supply to cover the possibility of supplier failure.

2.43 The Office for Government Online has not responded fully to the recommendations from the ANAO's previous audit pertaining to the provision of advice to Commonwealth bodies about managing purchasing risks. Commonwealth bodies are individually responsible for managing their Year 2000 purchasing risks and ensuring business continuity in the face of potential interruptions in the supply of business critical goods and services. Nevertheless, Commonwealth bodies could benefit from the provision of practical advice about better practices utilised by public and private sector organisations to manage Year 2000 supply chain risks. The whole-of-government management of supply-chain risks would be assisted by raising industry awareness of the Commonwealth's requirements as a purchaser of a range of essential goods and services.

Recommendation No. 1:

2.44 ANAO recommends that the Department of Communications, Information Technology and the Arts, through the Office for Government Online:

(a) identify and encourage the application by Commonwealth bodies of better practices in relation to the effective management of Year 2000 risks to the supply of essential goods and services; and

(b) formulate strategies to raise industry awareness of the Commonwealth's requirements in relation to the management of its Year 2000 risks.

2.45 Selected Commonwealth bodies responded to the recommendation as follows:

- ***Agree:*** Airservices, ATO, Centrelink, Customs, Defence, DETYA, DIMA and OGO (1a).
- ***Agree with qualification:*** OGO (Recommendation 1b).

2.46 Specific Comments by selected Commonwealth bodies are set out below:

- **OGO Response:** Agree with recommendation (1a) and agree with qualification to recommendation (1b). The Office for Government Online (formerly OGIT) advises that it will continue to share information from other organisations on best practices in relation to the effective management of Year 2000 risks to the supply of essential goods and services through its on-going communication activities. In relation to recommendation 1(b), OGO advised that Commonwealth bodies are individually responsible for managing their Year 2000 supply chain risk and ensuring business continuity. OGO noted that in all standard Commonwealth common-use contracts for the provision of supply and services, there are clauses relating to the Year 2000 issue. OGO has sought information from all utility suppliers to the Commonwealth about Year 2000 compliance. OGO indicated that it will continue to raise with industry the Commonwealth's requirements for essential goods and services so that it can manage its Year 2000 risks.

2.47 **ANAO Comment:** The ANAO acknowledges that Commonwealth bodies are individually responsible for managing their Year 2000 supply chain risk and ensuring business continuity. However, the ANAO has observed that Commonwealth bodies—including a number of those reviewed for this audit—desire advice and guidance concerning the most effective methodology(ies) and approach(es) to the analysis and management of Year 2000 supply chain risks. The ANAO considers that contractual provisions alone may not confer adequate protection in the absence of a robust analysis of an organisation's key product dependencies. It is possible that, for many bodies, the analysis of product dependencies will be an unfamiliar discipline and that there would be benefit in collating and disseminating information about relevant better practices.

Utilities

2.48 In the previous audit, the ANAO concluded that the then OGIT was best placed to coordinate a single approach on behalf of the Commonwealth to seek assurance about the continued supply of telecommunications, electricity, water and sewerage services.[60] The ANAO

[60] Op. cit., ANAO, Finding and Recommendation No. 3, pp. 22-23.

recommended that OGIT, on behalf of the Commonwealth, seek written assurances about Year 2000 compliance from utility suppliers in each State and Territory and communicate the outcomes to agencies. OGIT agreed to the recommendation and advised that it was working with State and Territory agencies to develop a coordinated approach to utility companies.

2.49 In February 1998 OGIT wrote to utility service providers seeking information on their progress to become Year 2000 compliant. OGIT requested and verified contact details about utility suppliers from State and Territory Government officials.[61] In October 1998 OGIT made further direct representations on behalf of the Commonwealth to utility suppliers in each State and Territory. Utility suppliers were requested to complete and submit a summary quarterly report on their progress in addressing the Year 2000 problem.

2.50 Each of the selected bodies reviewed for this audit is concerned to establish the likelihood of the interruption of utility services. Although OGO has placed a summary of the results of its initial request for information[62] in the restricted area of its Year 2000 website, selected agencies consider that the statements offered by utility suppliers fall short of providing the assurance they require concerning the risk of service interruptions. As a result, many bodies have acted independently to seek confirmation about the compliance of utilities.

2.51 Although the Commonwealth is, in aggregate terms, a major consumer of utility services, with the exception of telecommunications where there is still significant market concentration, it purchases utility services from a large number of public and private sector suppliers. This means that the Commonwealth's buying power may not be sufficiently concentrated to enable the exertion of significant market leverage, especially in relation to services for which alternative sources of supply may not be readily available or which utilise common infrastructure.[63]

[61] The then OGIT initially took the view that this was a matter which should be addressed through liaison with State and Territory officials. However, Victorian Government officials declined to provide a list of utility suppliers and, as a result OGIT did not directly contact Victorian utility suppliers in its first round of correspondence.

[62] Approximately two thirds of the utility suppliers contacted responded to the initial inquiry.

[63] The Chairman of the National Year 2000 Steering Committee wrote earlier this year to the (then) Minister for Industry, Science and Tourism to highlight the potential risks to business and industry of any interruption in the supply of utility services. Subsequently, the Minister wrote to Premiers and Chief Ministers to suggest a sectoral approach wherein publicly-owned utilities would provide regular reports to responsible State or Territory Ministers indicating, among other things, proposed timetables for achieving compliance. The Minister also suggested where there is significant private ownership, a whole-of-sector approach could be taken of either a consultative or a regulatory nature. The Minister also wrote to relevant Ministers to encourage reporting on a whole of sector basis on the status of Year 2000 readiness in the banking and financial services, communications, and airports and air traffic control sectors respectively. For its part, the National Year 2000 Steering Committee has no mandate to directly seek assurances from utility suppliers on behalf of either the Commonwealth or the business community.

2.52 The Commonwealth has minimal regulatory authority in relation to utilities other than telecommunications.[64] Furthermore, the options available to Commonwealth bodies within their existing administrative and statutory authority are limited (and are generally consistent with the actions and remedies available to private sector organisations). For their part, utility suppliers may be reluctant to disclose the full detail of their Year 2000 preparation for commercial and legal reasons. For these reasons, Commonwealth bodies will need to continue to communicate with relevant utility providers, carefully analyse the likelihood and potential impact of an interruption on the supply of utility services and give consideration to possible contingency arrangements.

2.53 **Finding:** The continued supply of essential infrastructure services such as telecommunications, electricity, water and sewerage is a matter of vital concern to Commonwealth bodies and the community generally. Interruptions in the supply of these services could impair the delivery of key government functions and entail significant financial and human costs. No analyses have been prepared for the Commonwealth examining the likelihood of service interruption, possible impacts or whole-of-government contingency options. The ANAO found that the Office for Government Online has had limited success in obtaining information from Australian utility suppliers and that the information provided to date falls well short of a guarantee of continuous service delivery. OGO is continuing to seek clarification about utility suppliers' Year 2000 status on behalf of the Commonwealth, but has no authority to compel non-Commonwealth-owned utility suppliers to respond to requests for information. In addition, selected bodies have independently requested information from utility suppliers. The ANAO notes, however, that Commonwealth bodies also have no authority to compel the provision of information by utility suppliers and the matter of continuity of supply is largely an uncontrollable risk.

Recommendation No. 2

2.54 ANAO recommends that the Department of Communications, Information Technology and the Arts, through the Office for Government Online:

[64] The exception to this is the Snowy Mountains Hydro-electric Authority (SMHA), a Commonwealth statutory authority. The Authority is in the process of being corporatised to work within the newly formed National Electricity Market as a self-supporting corporation jointly owned by the Commonwealth, New South Wales and Victorian Governments in ratios equal to their existing electricity entitlements (13 per cent, 58 per cent and 29 per cent, respectively). Source: *http://www.snowyhydro.com.au:80/ corpinfo/profile.htm*

(a) continue making direct approaches to utility suppliers and complement these actions with approaches to relevant representative industry bodies and regulatory authorities; and

(b) together with relevant lead agencies, coordinate the preparation of a risk analysis of the potential for the interruption of utility services and assess the potential impacts on key government services.

2.55 Selected Commonwealth bodies responded to the recommendation as follows:

- *Agree* Airservices, ATO, Centrelink, Customs, Defence, DETYA, DIMA and OGO (2a).
- *Agree with qualification:* OGO (Recommendation 2b).

2.56 Specific Comments by selected Commonwealth bodies are set out below:

OGO response: Agree with recommendation (2a) and agree with qualification to recommendation (2b). OGO agreed with qualification on the basis of the following strategy that is being implemented by OGO; notwithstanding that service continuity is the responsibility of individual agencies. The strategy is for OGO to: develop guidelines for contingency planning; seek progress details from utility service providers; arrange workshop(s) to address specific issues in relation to potential risks to the delivery of key government services; disseminate information on potential risks through on-going communication activities to Commonwealth bodies; and ensure that agencies that provide key government services have the necessary contingency plans in place.

2.57 **ANAO Comment:** ANAO recognises that the activities identified in the OGO strategy are important and necessary, however, they do not, alone, serve to fulfil the intent of the recommendation. Specifically, the recommendation calls for OGO to utilise a lead agency approach, as articulated in OGO's Corporate Goal, Objectives and Principles[65], to prepare a risk analysis on a whole-of-government basis in order to advise the Government about the likelihood and potential impact on key Government services of any failure of essential utility services. This could take a number of forms, including commissioned research in relation to the Year 2000 risks inherent in the design, engineering, structural and market characteristics of key utility industries (utilising published data).

[65] These state that OGO will promote and support the lead agency concept, preserve individual and cross agency responsibilities for projects in their respective sectors and *support agencies that have particular skills or roles to develop solutions which have wider applicability across government* (Source: http//www.ogit.gov.au/aboutOGIT/goal.html#OGITsCorporateGoal).

Continuity management

2.58 Continuity management in the public sector refers to management and planning for the continued availability of services to the Government and the public, including all the functions and resources associated with the provision of services.[66] Continuity management is a logical extension of Commonwealth bodies' corporate planning and risk management practice and requires leadership and the application of strong project management and risk management disciplines.[67] Continuity management enables the identification and assessment of risks which could disrupt Government services and functions, predict likely problems, and plan for the avoidance or minimisation of impact should problems occur.[68] Continuity management consists of a series of key elements, including the development of a risk management plan, implementation of a risk reduction plan and the development of contingency plans. Contingency plans, in turn, require the development of emergency response and resumption plans (see Figure 2.2).

2.59 Under previous Finance Directions heads of Commonwealth bodies were required to develop and implement continuity management plans.[69] Although these directions have since been superseded by the introduction of Orders and Regulations under the *Financial Management and Accountability Act 1997*, and express directives in relation to continuity management arrangements are no longer in force, continuity management planning remains an important element of sound management practice.

2.60 In September 1997, the Minister for Finance and Administration and the Minister for Science and Technology announced that the Government was working with Emergency Management Australia (EMA)[70] *to ensure that we have Year 2000 contingency plans in place should essential infrastructure, such as telecommunications, gas, electricity and water, experience problems at the turn of the century.*[71] Although the continued provision of

[66] Non-stop Service: Continuity Management Guidelines for Public Sector Agencies, Emergency Management Australia, 1997, p vii.

[67] Ibid., p. viii.

[68] Ibid. , p. 1.

[69] Direction 34(24A) required the formulation, implementation and testing of procedures to minimise the likelihood of a preventable disaster and, in the event of a disaster, minimise its impact on operations and services. Direction 34(24) required appropriate arrangements be made to copy and store system software, production data and essential records to enable the regeneration of business systems and records should a disaster occur.

[70] Emergency Management Australia is part of the Department of Defence and provides national emergency services coordination.

[71] Joint Media Release (51/97), Minister for Finance and Administration and the Minister for Science and Technology, National Strategy for the Year 2000 Computer Bug, 12 September 1997.

essential infrastructure, such as utility services, should be a priority in any continuity management planning, it needs to be recognised that there are other sources of potential risk to the continuity of Government services. OGO has advised the ANAO that it is currently developing Year 2000 contingency planning guidelines in consultation with lead agencies.

2.61 The importance of Commonwealth bodies undertaking continuity management and contingency planning in relation to Year 2000 is discussed in chapter four. However, selected bodies generally agree that it may be necessary to integrate and harmonise continuity management and contingency plans within a whole-of-government context with the objective of planning for the continuity, and if required, the resumption of key government services.[72] This might be more efficiently and effectively achieved if coordinated by an appropriate central agency, such as OGO.

2.62 A key element of contingency planning undertaken by Commonwealth bodies or at a whole-of-government level will be the development of appropriate communication strategies targeting clients, stakeholders and the community generally. The object should be to provide reassurance about the Commonwealth bodies' actions to achieve Year 2000 compliance, address client and stakeholder concerns about service continuity and provide information about contingency measures.

2.63 **Finding:** The ANAO considers that there is a need for the development of whole-of-government continuity management and contingency plans in order to avoid or minimise the disruption of key Government functions and services. Such action would be in line with the Government's statements concerning the development of contingency plans to deal with potential interruptions of essential infrastructure. The ANAO found that corporate continuity planning processes have been well

[72] In an interactive satellite television discussion convened in Canberra by the United States Information Service on 27 October 1998, John Koskinen, Assistant to the President and Chair of the President's Council of Year 2000, stated that the US Federal Government is developing contingency plans for those aspects of the Year 2000 problem requiring a Federal response. An overall contingency plan for the US is being formed, including the establishment of a central command centre to coordinate emergency response services and manage competing demands for limited resources. Koskinen also reported that the US is also working with the United Nations to convene a UN session on international contingency planning involving national Year 2000 coordinators to be held in New York on 11 December 1998. The session will be convened by a Steering Group of the UN Informatics Working Group and will focus on contingency planning at the country level and on issues affecting global financial transactions. There is a growing recognition of the need to manage international Year 2000 interdependencies. In a recent article in the OECD Observer (No. 214 October/November 1998) Vladimir López-Bassols, of the OECD Directorate for Science, Technology and Industry, observed that *given the interdependence of economies and the potential for cross-border disruption from the year 2000, international initiatives are needed to coordinate remediation, testing and contingency planning, especially for developing countries where awareness of the issue remains low and action is lagging* (pp 22-23).

articulated and are available to Commonwealth bodies to guide the development of continuity management and contingency management plans. The Office for Government Online (and previously, OGIT) has acted to raise Commonwealth bodies' awareness of the continuity management guidelines published in 1997 by Emergency Management Australia. The ANAO notes that OGO is also preparing Year 2000 contingency planning guidelines in consultation with lead agencies.

2.64 Communication strategies will be an important element of continuity management arrangements for individual Commonwealth bodies. These may comprise messages designed to manage stakeholder perceptions of the Year 2000 risks to services as well as communication strategies for the provision of public advice or instruction in the event of any interruption of services. The ANAO considers that communication strategies need to be coordinated at a whole-of-government level in order to reduce the potential for confusing or contradictory public messages; to avoid potential adverse effects of unintended messages; and to inform the community about the actions being taken to ensure the continuity of key government services.

Recommendation No. 3

2.65 ANAO recommends that the Department of Communications, Information Technology and the Arts, through the Office for Government Online:

(a) convene urgent discussions with relevant Commonwealth bodies to identify and provide advice to Government on aspects of the Year 2000 problem which require a whole-of-government approach to continuity management; and

(b) consult relevant Commonwealth bodies in the development of appropriate communication strategies to inform clients, stakeholders and the community generally about arrangements for continuity management in relation to key Government functions.

2.66 Selected Commonwealth bodies responded to the recommendation as follows:

- ***Agree:*** Airservices, ATO, Centrelink, Customs, Defence, DETYA, DIMA and OGO.

Figure 2.2
Continuity Management Guidelines

Year 2000 is one of a number of possible events which has the potential to disrupt Government services. Therefore, contingency arrangements for possible Year 2000 events need to be addressed within an overall continuity management framework. Guidelines produced in 1997 by Emergency Management Australia describe a continuity management process comprised of four phases complemented by structures for ongoing maintenance and review:

1. ***Initiation and project management*** (involving awareness raising, gaining management commitment and establishing a continuity management project*);*
2. ***Development of a risk management project*** (involving corporate risk analysis, risk identification, impact analysis and risk reduction options);
3. ***Implementation of a risk reduction plan*** (involving selection of risk reduction strategies, preparation and implementation of risk reduction plans); and
4. ***Development of Contingency Plans*** (including the development of emergency response plans and resumption plans).

Among the various sources of *credible risk* identified by Emergency Management Australia are *technological hazards* which *may originate from industry and the failure of social infrastructure and technical systems*. Emergency Management Australia includes among technological hazards *systems failures related to office equipment, information systems, (eg. from computer viruses, the Year 2000 date change), utilities (power, water, telecommunications, sewerage), industrial sites (sources of chemical, biological an nuclear hazards), building and community infrastructure and transportation.*

Contingency planning is defined as a *continuity management strategy* for dealing with *residual risks* by enabling the implementation of procedures to reduce the immediate impact of emergencies or disasters (emergency response plan) and recover services with minimal disruption (resumption plan). Contingency plans should be built upon the information provided by risk management processes and impact analysis including information in relation to: a listing of services in order of criticality for resumption; potential sources of disruption, areas of impact and effectiveness of existing safeguards; and resources, functions and services most at risk of being unavailable.

Emergency response and resumption plans should be:

- capable of being implemented on any day of the year, at any time of day and under all weather conditions;
- based on routine agency arrangements and organisational structures;
- integrated with other plans and activities across the organisation and coordinated with relevant external organisations and authorities; and
- sufficiently flexible to cover a wide range of possible sources and levels of risk.

Contingency planning needs to address: staff and visitor health and safety; direct clients and stakeholders; the community; suppliers; assets and resources (including facilities and buildings; information and records; and equipment); performance (in terms of quality and timeliness); and intangibles such as reputation, good will and confidence.

Source: *Non-Stop Service: Continuity Management Guidelines for Public Sector Agencies*, Emergency Management Australia, 1997.

3. Identification, planning and management of Year 2000 risks

This chapter examines the extent to which selected Commonwealth bodies have established core planning and project management elements; compiled inventories of affected systems; and assessed likely impacts and are appropriately managing Year 2000 resource requirements.

Background

3.1 The audit focussed on Commonwealth bodies' governance of their Year 2000 projects and, in so doing, consideration was given to *inherent* and *project* risks. Inherent risks refer to the range of factors which contribute to an organisation's overall exposure to the Year 2000 problem. Inherent Year 2000 risks may be present in the characteristics of Commonwealth bodies' business environment, utilisation of technology, management culture or organisational structure. Project risks refer to factors which adversely affect the coordination, continuity, effectiveness and accountability of bodies' Year 2000 projects and thereby militate against the achievement of, or assurance about, Year 2000 compliance. These may include factors such as inadequate governance structures, ineffective resource allocation or insufficient project management disciplines.

3.2 Each of the Commonwealth bodies reviewed for the current audit represents relatively high levels of inherent risk by virtue of the nature and importance of their functions, their dependence on IT-enabled business processes, their organisational and business complexity, and their exposure to potential institutional and structural change. In addition, each of the bodies examined differs in terms of the mix and salience of inherent risk factors. The following examination focuses primarily on issues of *project* risk factors, largely because these are the most directly observable and auditable features of an organisation's Year 2000 task. However, the ANAO's analysis has also taken into consideration the inherent risk factors confronting each of the bodies reviewed. In particular, chapter five addresses Year 2000 risks arising from organisational change and examines the potential for changes in inherent risk factors to have consequential effects on the continuity of Commonwealth bodies' Year 2000 projects.

3.3 The ANAO engaged the then Coopers & Lybrand[73] to assist with the identification of the essential project management elements and better

[73] Now *PricewaterhouseCoopers*.

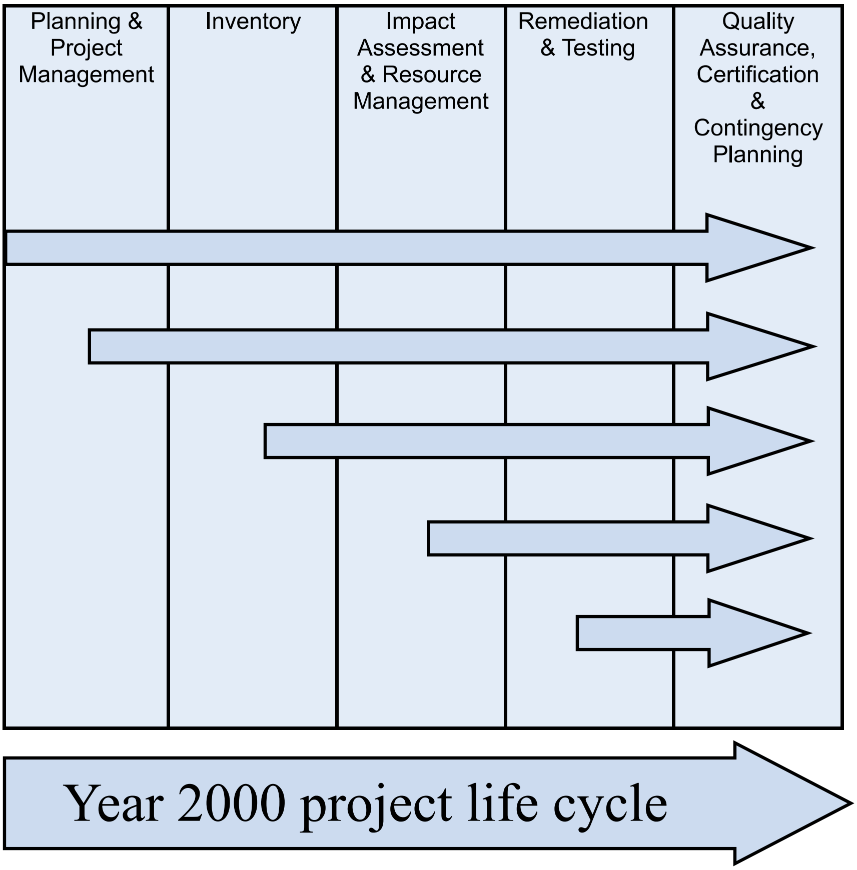
practice milestones for the completion of different phases of Commonwealth bodies' Year 2000 projects. While no single methodology can apply to all Year 2000 projects, most Year 2000 projects in large organisations can typically be broken into the following five phases of activity:

- planning, project management and risk management;
- compilation of inventories of affected business inputs;
- impact assessment and resource management;
- remediation and testing; and
- quality assurance, certification and contingency planning.

3.4 These phases need not be progressed sequentially and all will remain active to some degree from the point of commencement to the end of the project (which may continue beyond 2000). This is illustrated in Figure 3.1.

Figure 3.1

Year 2000 Project Life Cycle


Planning & Project Management
Inventory
Impact Assessment & Resource Management
Remediation & Testing
Quality Assurance, Certification & Contingency Planning
Year 2000 project life cycle

Source: ANAO based on advice from PricewaterhouseCoopers.

3.5 Each phase of activity may be further broken down into a series of project elements and milestones which are representative of accepted "better practice". The simplified set of "better practice" project elements are addressed in this chapter and in chapters 4 and 5.

Previous audit recommendations

3.6 The ANAO's previous audit recommended that Commonwealth bodies:

- review and document their Year 2000 assessment and planning activity to ensure that management can make a confident assessment of the appropriateness and sufficiency of their approach from a whole-of-business perspective;[74]
- establish appropriate mechanisms to ensure effective governance of their Year 2000 activities and to provide appropriate assurances to stakeholders in relation to the business implications of the Year 2000 problem, including assurances to stakeholders about the use of resources; efficient operations; financial integrity and validity; compliance with legislation; accountability to clients and other stakeholders; and public safety and security;[75]
- develop and document, as part of their overall risk management approach, a strategy for the management of Year 2000 risks that incorporates an analysis of the aspects of the operating, compliance and external environment that are potentially affected by the Year 2000 problem; the identification of possible sources of risk; an assessment and ranking of risks; options for the treatment of identified risks; and measures to monitor and review identified risks; [76]
- review their Year 2000 project management and take remedial action to ensure that the project is governed by clear and achievable milestones which are regularly reviewed; all staff responsible for aspects of the Year 2000 project operate within clear authorities and lines of accountability; and the project has top level commitment, including for adequate resources and strategic direction; [77] and
- establish a monitoring framework for their Year 2000 projects including independent review where considered appropriate; linkage with key corporate control systems; mechanisms which assure accountability for

[74] Op. cit., ANAO, Recommendation No. 4, p. 38.

[75] Ibid., Recommendation No. 5, p. 42.

[76] Ibid., Recommendation No. 6, p. 54.

[77] Ibid., Recommendation No. 7, p. 58.

the implementation of the Year 2000 project on time and within cost and quality parameters; and internal and external reporting arrangements to monitor progress against key project milestones which are regularly reviewed.[78]

3.7 **Finding:** The ANAO considers that the Year 2000 projects in each of the eight Commonwealth bodies reviewed for the current audit demonstrate, to varying degrees, qualities which are consistent with the recommendations from the previous audit.

Planning, project management and risk management

3.8 The current audit examined the extent to which bodies have established key project management elements and appropriate control mechanisms to govern their Year 2000 projects. The ANAO took into account the project structure, reporting relationships and the management of project information. The ANAO examined the extent to which selected Commonwealth bodies have:

- formed a project team;
- established project objectives;
- defined a project work plan;
- assessed Year 2000 risks; and
- determined risk mitigation strategies.

3.9 The ANAO considers that, by mid 1998[79], all Commonwealth bodies need to have substantially completed their Year 2000 project and risk management planning for all business areas. In addition, all Commonwealth bodies need to have established mechanisms to ensure regular and effective monitoring by senior management.

RBA, Centrelink, DETYA and Customs

3.10 The RBA, Centrelink, DETYA and Customs have generally established comprehensive management and control frameworks to guide and provide assurance about the progress of their Year 2000 activities. These bodies demonstrate a sound understanding of the Year 2000 problem, have comprehensively assessed their Year 2000 risks and have established the project management and control structures necessary to achieve their objectives.

[78] Ibid., Recommendation No. 8, p. 62.

[79] The nominated activities and program elements are those which the ANAO considers should have been completed and/or well established in Commonwealth bodies at the time of the commencement of audit field work in mid 1998. Many of these activities and project elements will have been completed and/or established *prior* to mid 1998 as stipulated in the Government's *Indicative Year 2000 Target Dates*.

3.11 At the time field work was conducted in June-July 1998, the level and quality of internal compliance with Year 2000 planning, assessment, documentation and reporting requirements was uneven among business units in each of these bodies. Variability in the quality of information available at the business unit level was largely compensated, however, by the extent and quality of communication between Year 2000 project personnel and business unit personnel. In each of these bodies, Year 2000 project personnel have a current understanding of each business unit's progress towards the achievement of key Year 2000 milestones. In addition, their Year 2000 project priorities were based upon a reliable assessment of the relative business importance of the systems and applications for which each business unit is responsible and the respective contribution of each system/application to the body's overall business effort.

DIMA, Airservices and ATO

3.12 DIMA, Airservices and ATO have each established project management and control frameworks for their respective Year 2000 projects. Year 2000 Project personnel in each of these bodies demonstrate a sound understanding of the Year 2000 problem and the associated business risks. Each body has put into place governance and control frameworks which are capable of supporting the provision of assurance about progress towards Year 2000 compliance and each has demonstrated progress in resolving systemic problems affecting their ability to monitor and confirm activity at the business unit level.

3.13 However, in each of these bodies, the ANAO was concerned that there appeared to be some inconsistencies in relation to: business units' understanding of the Year 2000 issue; the acceptance of relevant accountability for the management of Year 2000 issues at the business unit level; and/or business units' demonstrated compliance with internal reporting and control frameworks.

3.14 Although the factors that contributed to these impressions varied between these bodies, each utilises a management approach based upon devolved authority within an overarching business framework. In each of these bodies Year 2000 responsibilities are largely distributed to business units and Year 2000 Project coordinators have used a facilitation rather than an intervention approach. In DIMA's case, its Year 2000 project management and control framework had only recently been established at the time field work was undertaken and was being consolidated. In Airservices, action has been taken action to strengthen the management of its Year 2000 Project and improve internal compliance with reporting requirements. The ATO has sought to improve Year 2000 project monitoring and reporting through the implementation of software which provides an on-line management tool that can be remotely accessed by Year 2000 project managers at the business unit level.

Defence

3.15 Although Year 2000 planning activity has been under way in Defence since late 1996, a Year 2000 Project Office with broad coordination responsibilities was not established until December 1997.[80] At the time field work was undertaken, Defence had identified and was in the process of addressing problems with the coordination of Year 2000 activity within and between programs. Overall Year 2000 effort is being consolidated and Year 2000 project and risk management planning in mission critical areas has been accelerated.

3.16 Unlike other bodies assessed by this audit, Defence programs operate with a high degree of autonomy and this, combined with the size and complexity of the Defence portfolio, makes the task of portfolio-wide coordination and verification difficult. The Year 2000 Project Office has had success in raising the level of awareness about Year 2000 priorities as well as focussing and improving program-level efforts and reporting. The Year 2000 Project Office has also been required to assist with the resolution of inefficient communication within and between programs which has contributed to uncertainty and lack of clarity about specific Year 2000 accountabilities.

3.17 Defence acknowledges that internal coordination between sub-program elements in its Corporate Information Program (CIP)[81] has not been effective. As a consequence, Defence has implemented revised management arrangements and has applied additional contractor resources to put into place a coherent overall project management framework for CIP. Communication between other key programs and sub-programs is generally effective and constructive. Although there is a small number of areas where there is outstanding uncertainty about boundary or demarcation issues, it appears that these are being constructively resolved.

[80] The Defence Year 2000 Project Office was not established until December 1997 and a Year 2000 Project Implementation Plan was not prepared until June 1998. Prior to the establishment of the Year 2000 Project Office, Year 2000 activity was being progressed by individual program areas with little effective coordination.

[81] The Corporate Information Program (CIP) is the technical authority for key Defence business systems - such as the Standard Defence Supply System (SDSS) and the Defence Financial Management Information System (DEFMIS) - which are essential to the delivery of Defence's logistic capability. CIP also includes critical sub-programs such as: the Defence Computing Bureau (DCB), which is responsible for the delivery of mainframe computing platforms; the Defence Network Services Group (DNSG), responsible for base area communications and desk top systems; and, the Defence Communication Group (DCG), responsible for wide area data and voice communications. DCB, DNSG and DCG each provide vital elements in Defence's logistic and business systems.

3.18 Overall the situation in Defence is improving, particularly in programs and sub-programs identified by Defence as being *mission critical*.[82] By contrast, non-mission critical areas have not shown a similar level of improvement. In general, it would be prudent for Defence executive management to closely monitor the effectiveness of internal communication about Year 2000 matters. In particular, the delineation of responsibility between program and sub-program elements needs to be closely monitored and mechanisms established to identify the potential transfer of risks and resolve disputes.

3.19 **Findings:** The ANAO found that in the Reserve Bank of Australia; the Department of Education, Training and Youth Affairs; Centrelink; and the Australian Customs Service**:**

- coherent and effective Year 2000 project management frameworks have been established with strong governance structures and controls;
- year 2000 project and risk management planning have been substantially completed and covered all business areas; and
- mechanisms have been established to ensure regular and effective monitoring by senior management.

3.20 Year 2000 project management frameworks, governance structures and controls, project and risk management planning, and project monitoring are also features of the Year 2000 projects in Airservices Australia, the Australian Taxation Office; the Department of Immigration and Multicultural Affairs; and the Department of Defence. However, circumstances were observed in each body which led the ANAO to qualify its findings.

3.21 Airservices Australia acted relatively late to implement strategies to recover from Year 2000 project delays experienced as a result of insufficient initial resourcing. Airservices' Year 2000 efforts have accelerated significantly since March 1998 and a number of important project management elements have been enhanced. Year 2000 project and risk management planning has been substantially completed and covers all business areas. Mechanisms have been established to ensure regular and effective monitoring by senior management.

3.22 In the Australian Taxation Office Year 2000 project and risk management planning has been substantially completed and covers all business areas. Formal governance arrangements provide a sound control framework for its Year 2000 activities. Weaknesses were observed in relation

[82] The term 'mission critical' pertains to Defence's ability to raise and sustain a military *mission*. Mission capability is considered by Defence as its core business, which is to say, 'warfare capability'.

to business units' internal compliance with ATO's Year 2000 reporting and control framework. In mid 1998 the Australian Taxation Office implemented an on-line management tool which should go some way towards improving compliance and verification.

3.23 The Department of Immigration and Multicultural Affairs' Year 2000 project commenced relatively late and required accelerated effort. This delay, coupled with the implementation of IT outsourcing arrangements and other organisational changes, suggest that DIMA's Year 2000 Project is still in a consolidation phase and will need to be monitored.

3.24 The Department of Defence established its Year 2000 Project Office in December 1997, and mechanisms have been implemented to ensure regular monitoring of Year 2000 activities. At the time field work was undertaken, Defence had identified and was in the process of addressing problems with the coordination of Year 2000 activity within and between programs. Overall Year 2000 effort is being consolidated and Year 2000 project and risk management planning in mission critical areas has been accelerated.

Compilation of inventories of affected business inputs

3.25 The audit examined the extent to which bodies have compiled detailed inventories of potentially affected business systems, applications and services for each aspect of their operations[83] and assessed the extent to which the preparation of inventories reflected the following key project elements:

- all resources that support critical functions have been identified;
- all internal and external interface relationships have been identified;
- all key business processes are documented and understood; and
- key supply chain partners and data interface partners have been documented.

3.26 The ANAO considers that, by mid 1998[84], Commonwealth bodies need to have compiled detailed inventories of all supported and user-maintained IT systems and applications across all business areas and to be in the process of compiling an inventory of non-IT (embedded) systems.

[83] Including hardware and software items (including embedded systems), IT vendors, business partners and relevant contractual relationships.

[84] As stated in footnote 79 the nominated activities and program elements are those which the ANAO considers should have been completed and/or well established in Commonwealth bodies at the time of the commencement of audit field work in mid 1998.

By the end of 1998, comprehensive inventories of IT and non IT business elements need to be well established and subject to robust control processes to ensure their continuing accuracy. Inventories need to be structured to allow business risk analyses to be performed and need to be regularly updated.

3.27 Inventory control, in the context of an organisation's Year 2000 project is an important input into its Year 2000 risk management. The confirmation or verification of IT inventories is a continuous process. Inventories are regularly adjusted to reflect changes flowing from the addition, retirement or replacement of applications and systems. This requires the application of appropriate disciplines and inventory control systems.

RBA, Centrelink, DETYA and Customs

3.28 Inventories of IT systems and applications in RBA, Centrelink, DETYA and Customs are sufficiently comprehensive to provide an adequate basis for the assessment of key risk exposures and the articulation of appropriate risk mitigation strategies. These bodies have established reporting and control mechanisms which are effective in supporting the ongoing monitoring and revision of their inventories. Each of these bodies has substantially compiled its inventory of IT systems and applications during 1997 and, during the first half of 1998, directed its efforts towards the reconciliation of their inventories and the verification of the processes used for inventory control.

3.29 Year 2000 projects in each of the bodies exhibit a degree of central coordination and quality control in relation to inventories compiled at the business unit level. This level of central oversight also extends to assessing and moderating the level of priority or criticality assigned by business units to particular systems, applications, and classes of systems. Through this process, these bodies have arrived at a balanced assessment of the business criticality of major systems and applications from a whole-of-business continuity perspective.[85]

3.30 Each of these bodies operates in a dynamic environment and each has been required to manage significant new operational and administrative initiatives arising from government policy. Although these initiatives have competed for internal resources required by the bodies' Year 2000 projects, to differing degrees they have assisted the process of compiling, verifying

[85] It has been observed in a number of bodies that systems assessed as being business critical from a business unit perspective, may not have a high degree of criticality from a whole-of-business perspective.

and reconciling their systems inventories thus placing the bodies in a strong position to focus on achieving a compliant business environment.

3.31 In Centrelink, DETYA and RBA, changes in administrative arrangements have provided an enhanced impetus to clarify the ownership and responsibility for IT hardware and software assets.[86] In Customs and DETYA, the market testing and, in the case of Customs, outsourcing of IT functions provided added impetus to the confirmation and reconciliation of IT inventories as well as introducing external checks on the accuracy of inventories by the prospective contractor. In Customs' case, responsibility for the ongoing management of the IT inventory has been assumed by the IT contractor.

DIMA, Airservices and ATO

3.32 DIMA, Airservices and ATO have expressed confidence that their inventories of business critical IT items are complete and provide a sufficient basis for the identification of priorities, resource requirements and time frames for implementation. At the time field work was undertaken, the ANAO noted that DIMA[87] and Airservices[88] were in the process of implementing verifiable processes for the purpose of IT system inventory control. Confirmation of the accuracy and completeness of DIMA's IT inventory has been assisted by the decision in July 1998 to outsource IT infrastructure management and desk-top support.[89]

3.33 The ATO has expressed confidence that its inventory of business critical IT systems is complete. ATO business units have been required to identify the systems and applications within their control; assess the business criticality of inventory items; and, identify an application or product owner for each inventory item. The ATO's confidence derives from

[86] In Centrelink, this has occurred through the separation of the service delivery functions from the Department of Social Security in July 1997. In the former DEETYA, the replacement of the Commonwealth Employment Service with a new statutory entity, Employment National (May 1998) and in the RBA, the creation of the Australian Prudential Regulation Authority (July 1998) has required each body to clarify the ownership and Year 2000 status of IT assets relevant to the business continuity of each of the new entities.

[87] DIMA has subsequently advised the ANAO that it has now completed the identification of all resources that support a critical function.

[88] In April 1998, Airservices senior management expressed concern with the overall progress of the body's Year 2000 project, including a lack of clarity about the completeness of the IT inventories compiled by business units and the currency of the reported Year 2000 status of IT assets. In June 1998 Airservices replaced an existing, less detailed systems data base with an enhanced, centrally maintained on-line inventory data base.

[89] DIMA compiled its inventory initially in 1997.

the *normal management arrangements* in place for all of its application development and maintenance activity. The ATO reports that:

> *...as a matter of normal business, specific project management responsibilities exist within all business and service lines for all systems, not just [Year 2000] specific items. It is the inventories of these arrangements that in fact were used to derive the listing of 'mission critical' items that we are concentrating on for [Year 2000], and, as recently as May 1998 the Y2K Steering Committee asked that all [Business and Service Lines] confirm the inventory.*

3.34 It is considered that the on-line monitoring and reporting mechanism implemented by ATO in mid-1998 will better support the ongoing monitoring and revision of ATO's inventory than the oral and written mechanisms it replaced.

Defence

3.35 In Defence, business units (effectively, programs and sub-programs) are responsible for the preparation and maintenance of inventories of IT systems and applications. A number of Defence's enabling[90] programs have been assisted in this regard by contractors engaged by the Defence Year 2000 Project Office.[91] Defence reports that inventories of mission critical systems are largely complete, although inventories in a number of sub-program areas were in the process of being compiled and/or reconciled at the time field work was undertaken.

3.36 Until the establishment of the Year 2000 Project Office in December 1997, there was no formal central coordination mechanism for Defence Year 2000 activity. The relatively late implementation of a coordination function, combined with other management issues, has meant that in a number of programs, the documentation and verification of inventories is not as well advanced as it should be. Owing to the diversity and complexity of Defence's operations it has not been possible for the Year 2000 Project Office to independently confirm the accuracy of inventories compiled by each of the 14 programs. It is possible that further confirmation of existing IT inventories could reveal duplication and omissions.

3.37 Defence has successfully accelerated Year 2000 effort in mission critical areas and the Year 2000 Project Office is confident that all mission

[90] Defence programs are broadly divided into 'enabling' and 'capability' programs. Enabling programs are those which provide business services and other key support activities. Capability programs deliver 'defence capability' (or *warfare* capability) and are the major clients, or stakeholders, of enabling programs.

[91] The contractor has personnel placed in four Programs: Corporate Information, Support Command Australia, Defence Acquisition Organisation and Joint Education and Training.

critical systems have been identified. Defence acknowledges the potential for degradation of administrative efficiency and effectiveness in non-core programs (involving non-logistic business systems supporting human resource management or education and training areas[92]). Given the size of the organisation, the diversity of its business processes and the number of potentially affected systems, the observed delay in completing this phase of activity reduces the time available for remediation and testing. Strong portfolio level oversight will be required to keep Defence's overall Year 2000 effort on target.

Embedded systems

3.38 All of the selected Commonwealth bodies have formulated strategies to address Year 2000 risks to embedded systems.[93] As with IT systems and applications, it is necessary to compile inventories of embedded systems and to assess both their business importance and the extent to which they are affected by the Year 2000 problem. Each of the selected bodies recognises the need to address embedded systems risks. In RBA, Centrelink, DETYA, DIMA and ATO, the major embedded systems risks are to do with building systems (including fixtures such as lifts, environmental controls, security and safety devices and utility interconnections). The RBA reports that it has now compiled a comprehensive inventory of embedded systems and equipment in the Bank's facilities nation wide.

3.39 In Defence, and to a lesser degree Customs and Airservices, the range of potential embedded system exposures extends beyond building systems to include a range of specialist equipment containing electronic components whose operation may depend on calculations using year dates. In Defence, this includes a large variety and number of warfare assets utilised by the Navy, Army and Air Force (see Figure 3.2). Responsibility for the assessment and management of Defence warfare assets is shared between three programs: Support Command Australia, Defence Acquisitions Organisation and Navy (Maritime Command).

[92] However, these are unlikely to significantly affect mission capability. Some personnel systems could have an impact on mission capability insofar as they support the deployment of personnel. Defence is confident that appropriate work-arounds are available for business systems contributing to mission capability.

[93] Embedded systems refers to equipment containing microchips and/or firmware; process monitoring, control and data acquisition systems; or any other equipment and/or operating systems used to control the operations of equipment or machinery. Embedded systems are frequently used in manufacturing and building systems and are sometimes referred to as *non-IT*, principally because they are not generally included in the IT inventory.

Figure 3.2
Embedded System Risks in Defence

Of all Commonwealth organisations, Defence has perhaps the largest potential exposure to embedded systems. Of special concern, on the counts of defence capability and public and personal safety, are Defence's warfare assets, including land, sea and air vehicles (including fuel infrastructure and simulation systems for training purposes), navigation, flight control and locational devices, weapons systems, ordnance, communications devices and medical equipment.

In May 1998 the Defence Year 2000 Project Office commissioned a report on *Year 2000 Embedded System Issues for Defence Systems*.[94] The report observed that although defence systems are *normally the products of a disciplined process of design and engineering development* that takes into consideration *a range of stringent engineering standards*, the design of these systems *may not have considered Y2K rollover or other date/time representations, and comprehensive temporal testing may never have been performed*.

The report stated that *the management of a structured engineering approach to systems assessment, directed at ensuring fitness for purpose, is fundamental to ensuring the maintenance of operational capability,* and concluded that the prevalence of embedded systems in Defence does not necessarily translate into potential significant capability degradation. The reasons given in for this level of confidence are *the generally robust design characteristics of defence systems and the well developed engineering and support infrastructure that exists and aids the assessment and remediation of problems such as Y2K*.

Source: ANAO based on information provided by the Department of Defence.

3.40 Primary responsibility for the management of Year 2000 risks to Defence's *mission critical*[95] capability rests with Support Command Australia (SCA).[96] Within SCA, control systems and methodologies governing the identification and management of potential Year 2000 risks are clearly defined and understood. In addition, SCA maintains a high level of communication with other relevant Defence programs responsible for the management of Year 2000 risks to warfare assets. Defence has a high level of confidence about the 'fitness for purpose' of its warfare assets, based, in part, on its assessment of the design characteristics of the component

[94] Australian Maritime Technologies, Year 2000 Embedded System Issues for Defence Systems, 28 May 1998.

[95] See footnote 82.

[96] SCA is the program with major responsibility for addressing potential Year 2000 exposures in embedded systems for warfare assets used by the Army, Navy and Air Force. Sub programs SCA-Army, SCA-Navy and SCA-Air Force are, respectively, responsible for the assessment and remediation of all in-service equipment currently identified in the Standard Defence Supply System (SDSS), partially delivered acquisition projects and stand-alone PCs used for monitoring or control. In the case of SCA-Navy this specifically excludes naval operational combat systems (which are the responsibility of the Maritime Commander), although SCA-Navy is responsible for aviation assets (helicopters and flight simulators) and minor vessels. It should be noted that SCA is also responsible for identifying and resolving Year 2000 risks associated with medical systems and equipment in Defence hospitals and medical facilities. The Defence Acquisition Organisation (DAO) is responsible for ensuring the compliance of assets which are subject to acquisition and/ or which have not been fully commissioned and transferred to SCA or Maritime Command.

systems, and considers that mission critical capability is unlikely to be adversely affected by a Year 2000 failure in relation to warfare assets (defence materiel).

3.41 Defence acknowledges that its ability to sustain warfare capability over an extended period could be adversely affected by a degradation of logistics capability. Priority needs to be given, therefore, to assuring the integrity of logistics systems, in particular, through end-to-end testing in a fully integrated production environment. This should be the subject of contingency planning coordinated at the portfolio level.

3.42 In Airservices, non-building embedded systems include calibration equipment on leased aircraft and ground-based navigational aids while, in Customs, non-building embedded systems include vessels and detection equipment. Although by comparison with Defence, Airservices' and Customs' exposures to non-building embedded systems are low, these categories of equipment are nevertheless important to the performance of important business functions.

3.43 The compliance of many embedded systems cannot be directly tested and, for this reason, management must first obtain advice from suppliers and manufacturers.[97] Requests for advice about the compliance of embedded systems require long lead times and may require intensive follow-up.[98] Many suppliers and manufacturers may not themselves have an adequate understanding of the Year 2000 problem, may be reluctant to warrant the compliance of their products, or their representations about their products may be either ambiguous or unreliable.

3.44 Building systems may fail to function as a result of a date-related embedded system failure. Where bodies occupy leased premises, they are reliant upon building owners to confirm the compliance of building systems on their behalf. In some cases, selected bodies lease premises to other organisations and have received requests to confirm the compliance of building systems.[99] Some systems will be capable of being repaired while others may have to be replaced entirely. The ability of the market to respond to the demand for last minute solutions to building systems problems may

[97] Manufacturers, in turn, may need to seek advice from the suppliers or manufacturers of system components.

[98] Defence advises that it relies on established acceptance protocols to assess the Year 2000 risk to warfare assets affected by embedded systems (as distinct from building systems). Defence advises that advice from suppliers or manufacturers provides a starting point for further analysis based on engineering principles.

[99] Commonwealth bodies also occupy premises owned by the Commonwealth. At least one selected body has commented that confirmation of the Year 2000 compliance of building systems is more difficult to obtain for buildings leased from the Commonwealth than for buildings leased from the private sector.

be increasingly limited, and for this reason, it is important that Commonwealth bodies not delay their assessment of embedded systems risk.

3.45 Each of the selected bodies recognises the potential for building system failures to disrupt business, damage assets and present health and safety risks to staff and clients. However, in each of the bodies examined for this audit, efforts to establish the extent of risk posed by embedded systems in buildings has lagged behind actions to address risks to IT systems and applications.[100] Although the investigation of building related embedded system risks has commenced in each of the selected bodies, and responsibility for addressing various aspects of embedded system risk has been delineated, only RBA has completed its assessment. DETYA, Defence and Airservices, have engaged, or are about to engage, contractors with the specialist skills, industry knowledge and logistic capability to assist the inventory, assessment and remediation of building systems issues. DIMA reports that it does not own any property and is therefore *totally reliant on the assessments of building owners for risk assessment on embedded building systems*. DIMA considers this to be unacceptable and is investigating the option of engaging a consultant to carry out an independent risk assessment. The remaining bodies are managing this aspect of their Year 2000 problem largely in-house. [101]

Inventory of contracts

3.46 Selected bodies have not compiled inventories of all current contracts, largely due to the number and distribution of contracts across their organisations (and the consequent effort involved in compiling such an inventory). However, all of the selected bodies recognise the potential for legal risks arising through contractual arrangements for purchase and/ or supply of goods and services. Assessment of legal risk has occurred relatively recently and is ongoing. Each body has obtained legal advice on contractual issues.[102] Each body has reported a range of actions to address contracting risks including the incorporation of Year 2000 provisions in tender documentation, the inclusion of Year 2000 clauses in new or renewed contracts, and the adoption of purchasing guidelines designed to minimise exposure to third party risk.

[100] It should be noted that, in general, this has also been widely recognised as the case in the private sector.

[101] Some bodies such as DETYA and Customs use the services of commercial property managers which can address building systems issues on their behalf.

[102] Advice has been obtained either externally (through the Australian Government Solicitor or private legal firm) or internally through Commonwealth bodies' own legal counsel.

3.47 **Finding:** The ANAO found that in the Reserve Bank of Australia; the Department of Education, Training and Youth Affairs; Centrelink; the Australian Customs Service; Airservices Australia; the Department of Immigration and Multicultural Affairs; and the Australian Taxation Office**:**

- detailed inventories of all supported and user-maintained IT systems and applications have been compiled across all business areas; and
- IT inventories are subject to ongoing verification and reconciliation, are structured to allow business risk analyses to be performed and are regularly updated.

3.48 The Reserve Bank of Australia reports that it has completed its inventory of embedded systems while in Centrelink; the Department of Employment, Education, Training and Youth Affairs; the Department of Immigration and Multicultural Affairs; the Australian Customs Service; Airservices Australia; and the Australian Taxation Office, inventories of embedded systems are being compiled.

3.49 In the Department of Defence, mission critical systems have been identified and documented. Detailed inventories of less critical supported and user-maintained IT systems and applications are not complete, or have not been verified for all programs and sub-programs. Inventories of embedded systems affecting Defence establishments are being compiled with confirmation and assessment to be performed by a contractor with specialist expertise and necessary logistic capability. Inventories of embedded systems affecting warfare assets and medical equipment are largely complete and subject to further confirmation and assessment.

3.50 Selected Commonwealth bodies' investigations of embedded system risks affecting buildings and facilities has begun relatively late. In those bodies occupying a large number of establishments and buildings the assessment and remediation of affected systems may not be achieved within nominated time frames. Commonwealth bodies would be well advised to assess and prioritise their approach to facilities and building systems in terms of their potential impact on business continuity, security, the value of assets, occupational health and safety and public safety.

Fulfilment of statutory obligations

3.51 The possibility exists that Year 2000 systems failures may place Commonwealth bodies in breach of their legislation with the possible result of financial hardship for individuals and/or businesses. Although all bodies are aware of the potential for Year 2000 failures to adversely affect their ability to fulfil their statutory and regulatory obligations, it will be necessary for bodies to ascertain the likelihood of such an occurrence, quantify the possible liability for the Commonwealth and develop contingent operational, legal or policy options to limit their, and the Commonwealth's exposure. Regulators, in particular, may be required to consider the extent to which they might need to intervene in the affairs of regulated industries to ensure that they meet their legislative mandate. An example is presented in Figure 3.3.

Figure 3.3

Year 2000 preparedness and regulation of the banking sector

In recognition of the potential risk of disruption in the banking industry the RBA undertook a comprehensive survey of Australian Banks in May 1997 to assess the preparation of Australian banks for the Year 2000. At the time of the survey, banks compliance work was focussed internally and the RBA found that Australian banks' state of preparation was 'mixed'.[103] The first survey was followed up with a less detailed questionnaire in March 1998. The RBA indicated that the intention of the first survey was to raise awareness of the Year 2000 issue within the banking sector while the second was used to establish a benchmark for banking institutions' Year 2000 progress. Where survey returns raise concerns about a bank's actions to address the Year 2000 problem, the RBA initiates a discussion with the bank's senior management.

In July 1998, the RBA and the Australian Prudential Regulation Authority (APRA) jointly issued a booklet covering "Year 2000 Preparations in the Australian Banking and Financial System" This provided information on the above survey results, preparations in payments and settlements systems and the Bank's internal Year 2000 preparations.

As part of the prudential consultation process (from 1 July 1998 the responsibility of APRA), external auditors of the banks have been requested to provide detailed reports on each bank's continuity and contingency planning arrangements for Year 2000 and other risks. APRA has put into place a program of quarterly reporting for banks, with the first return outlining the status of preparations as at the end of September 1998. APRA has given the institutions the scope to complete their returns on a whole of business basis in order to better reflect the way in which the Year 2000 problem is managed in the organisation. Only one return is required for organisations which have more than one institution regulated by APRA. The results of this and further surveys will be published in an update to the July 1998 booklet *Year 2000 Preparations in the Australian Banking and Financial System*, which is available on the RBA's web site (*www.rba.gov.au/y2k*).

Source: ANAO based on information provided by the Reserve Bank of Australia.

Impact assessment and resource management

3.52 The audit examined the extent to which the selected Commonwealth bodies have analysed their inventories of affected systems, equipment, services and business dependencies to identify: the extent and likelihood of risk to their business critical operations; the likely impact(s) of any failure to successfully resolve their Year 2000 risk exposures; and resources required to provide solutions to identified problems.

[103] Deputy Governor, speech to Australian Institute of Banking and Finance Inc, 28 October 1997 (published in Reserve Bank of Australia Bulletin, November 1997, pp. 50-55).

3.53 The ANAO also examined the extent to which the selected Commonwealth bodies' impact assessment and resource management activities reflected the following key project elements:

- the prioritisation of business processes according to business continuity requirements;
- the prioritisation of technology for remediation according to business need;
- the assessment of project risks and identification of risk mitigation strategies;
- the confirmation of project scope and objectives with internal stakeholders; and
- the identification and commitment of necessary resources to remediate mission-critical systems.

3.54 The ANAO considers that, by mid 1998, Commonwealth bodies need to have comprehensively analysed potential business impacts for key business areas, assessed business priorities and determined resource requirements. By the end of 1998, the business impact assessment needs to be completed and robust mechanisms established to ensure that the assessment is able to be revised in accordance with dynamic project priorities based on ongoing risk assessment and quality assurance.

RBA, Centrelink, DETYA and Customs

3.55 The RBA, Centrelink, DETYA and Customs have taken a comprehensive view of their Year 2000 related business risk exposures. Each of these bodies has assessed potential business risks arising from the Year 2000 problem, identified critical internal and external business relationships and appropriately delegated business unit responsibility for managing key internal and external interfaces. Each has assessed the compliance status, event horizons[104] and business importance of their IT systems. In addition, each body actively monitors the progress of its remediation and testing effort, identifies emerging issues and regularly reviews Year 2000 resource requirements.

3.56 Year 2000 project staff in RBA, Centrelink, DETYA and Customs work closely with their respective business units, system/application owners and external partners on Year 2000 assessment, remediation and testing issues. DETYA and Centrelink have formalised reciprocal arrangements for the exchange of information and the coordination of

[104] Event horizon refers to the date on which a Year 2000 event will first occur: being the first occasion which requires a calculation or function using a 2000 date. This will be the date of first failure and may occur well before 2000.

testing. The RBA and Customs have formalised relationships with relevant industry groupings. In the case of RBA, this takes the form of the Interbank Working Group and a number of associated working groups while Customs participates in industry working groups convened to address business continuity issues at international airports.

DIMA, Airservices and ATO

3.57 DIMA, Airservices and ATO have each undertaken a high level business impact assessment although more detailed analyses of potential Year 2000 risks and impacts in relation to business critical systems and processes were still under way at the time fieldwork was carried out. Each has identified, and is closely monitoring its resource requirements and revising estimates in the light of information generated by ongoing assessment activity. Airservices has engaged a contractor to assist with the development of a comprehensive business risk assessment. DIMA is working with its *Strategic Partner* (the IT contractor) to analyse its business risks.

3.58 As with RBA and Customs, Airservices is working closely with its key external stakeholders and is engaged in a number of forums established to address airspace safety issues (see Figure 3.4).

Defence

3.59 Impact assessment is incomplete in some Defence programs and sub-programs. Assessment activity has been accelerated in programs and sub-programs responsible for mission critical systems and steps have been taken to address problems with coordination and communication. It has been observed that contractor resources contributed by the Year 2000 Project Office have had a significant positive effect in the programs where they have been applied.

3.60 Assessment, remediation and testing activities are occurring in parallel in a number of Defence programs. Although progressing the various phases of Year 2000 work in parallel will place greater demands on human resources, to the extent possible this will need to continue.[105] If this level of effort is to be sustained (and target dates adhered to) dedicated resources will need to be applied and competing internal resource demands will need to be managed. A number of program and sub-program areas have reported that their Year 2000 projects are affected by shortages of human and financial resources. Resourcing issues need to be carefully monitored and controlled. In particular, programs need to bring financial

[105] It should be noted that some sequencing of these activities is inevitable.

Figure 3.4
Addressing Airspace Safety Issues

In November 1997, Australia's two major airlines, Qantas and Ansett, convened a workshop to address business continuity risks at Sydney Airport. This workshop led to the formation of a number of focus groups comprising relevant government and industry participants addressing issues of airspace management, transiting aircraft and freight, and passenger and baggage movement. Airservices is a member of the airspace management focus group and will be working with other participants to identify all processes, information dependencies and responsibilities for addressing Year 2000 risks to airport operations.

The airspace management focus group covers all activities associated with controlling the use of airspace, including enroute navigation, flow coordination, flight control, flight tracking and monitoring, emergency services and manpower scheduling.[106] To assist discussions, Airservices has comprehensively mapped process flows in relation to departure, enroute and arrival sequences. All National Airways System (NAS) elements have been identified along with associated software dependencies, and internal/external interfaces. A priority rating and the Year 2000 status of each NAS element has been identified[107].

In June 1998, the Sydney Focus Group agreed to the formation of a National Steering Committee to be chaired by the Department of Transport and Regional Services (formerly Transport and Regional Development) which will facilitate a national perspective on airport and airspace safety issues. The National Steering Committee will operate alongside the Sydney Focus Group. An Air Traffic Management Sub-committee, chaired by Airservices, has been established. Airservices will continue its involvement with the airspace management focus group established under the aegis of the Sydney Focus Group.

Source: ANAO based on information provided by Airservices Australia.

resource concerns to the early attention of Defence's Year 2000 Project Office so that they may be resolved in a timely manner.

3.61 Findings: The ANAO found that in the Reserve Bank of Australia; the Department of Education, Training and Youth Affairs; the Department of Immigration and Multicultural Affairs; Centrelink; the Australian Customs Service; and the Australian Taxation Office:

- business impact assessment has been carried out for most business areas; and
- business priorities and resource requirements have been identified and documented.

[106] The membership of the group, in addition to Airservices, includes technical resources drawn from the Sydney Airport Corporation Ltd., Ansett Australia, Qantas, the Civil Aviation Safety Authority, SITA (Societe Internationale de Telecommunications Aeronautiques) and the Bureau of Meteorology. Meetings of the Focus Group have also been attended by the Royal Australian Air Force (RAAF).

[107] As at 21 May 1998, 24 NAS elements were identified of which two were listed as 'compliant', three were listed as 'ready for sign-off', one was listed as 'unknown' and the remainder were 'in progress'.

3.62 In Airservices Australia business priorities and resource requirements have been identified and documented. Business impact assessment has been carried out at a corporate, or global level with further business risk analysis to occur at the business unit, or local level.

3.63 In the Department of Defence, business priorities have been identified at the portfolio and program levels. Business impact assessments have been carried out to some degree for most business systems, with emphasis given to systems concerned with achieving and sustaining mission capability. Resource requirements have been identified and documented at a portfolio and program level. However, in some cases resource allocation could be better managed at the program level and it is not clear that all possible contingent requirements have been anticipated.

4. Remediation, compliance testing, certification and contingency planning

This chapter examines selected Commonwealth bodies' actions in relation to the remediation and testing of Year 2000 affected systems; and activities in relation to quality assurance, certification of compliance and contingency planning.

Remediation and testing

4.1 The audit examined the extent to which bodies have initiated remediation activities. The audit also examined whether remediation is managed efficiently and effectively, and whether remediation work is subject to formal quality processes. The ANAO took into account the extent to which remediation, testing and assurance activities demonstrate the following:

- quality assurance mechanisms have been established;
- the conversion, testing and implementation of business critical systems has commenced;
- the conversion, testing and implementation of other, less critical, systems has been scheduled; and
- assessment, testing and correction of embedded systems exposures has commenced.

4.2 The ANAO considers that by mid 1998, Year 2000 remediation should be under way with test programs established and quality control/ quality assurance processes applied to the remediation process. By the end of 1998, remediation should be complete for all critical systems with less critical systems being addressed subject to equivalent quality standards; test strategies should be in place, including appropriate control structures for the validation of test results and certification of compliance; and testing should be well under way for most business critical applications, systems and internal interfaces (see Figure 4.1). By mid 1999, all critical systems and most less critical systems should be compliant and certified as such by the executive management. In addition, all critical business inputs, business partners and potential supply chain risks should be identified; their Year 2000 compliance determined; and the level of residual risk comprehensively assessed.

Figure 4.1
Year 2000 Testing Activity

Testing is generally considered to be the most time consuming, costly and resource intensive phase of a Year 2000 project. It has been estimated that testing will require in the range of about 40 to 60 per cent of total Year 2000 effort. Testing involves a number of levels and phases (although not all levels and phases are applicable to all organisations) which may include:

- **Baseline Testing**—done before any changes are made to a system and used as a basis for comparison with later testing;
- **Unit Testing**—performed on changes at the individual program or module level;
- **Integration Testing**—tests interactions between software and/or hardware components;
- **System Testing**—all components are tested together;
- **Regression Testing**—tests the system using baseline test data to ensure that functionality remains sound;
- **User Acceptance Testing/Compliance Testing**—final testing for end user business functional requirements, and normally involves testing in a Year 2000 partitioned test environment;
- **Ongoing Maintenance Testing**—designed to ensure that maintenance activities do not adversely affect an already compliant program or system;
- **External Interface/End-to-end/Interoperability Testing**—to ensure the correct functioning of external interfaces with business partners, customers, suppliers and other persons with which the organisation exchanges data electronically; and
- **Embedded Chip/Non-IT Testing**—testing or confirming the compliance or fitness-for-purpose of equipment, machinery or physical plant whose operation is dependent on automated controls and/or microprocessors.

Source: Office of Government Information Technology, Year 2000 Testing Strategies, July 1998.

RBA, Centrelink, DETYA and Customs

4.3 The RBA, Centrelink, DETYA and Customs are confident that the remediation and internal integration testing of their business critical IT systems will be completed within the time frames generally accepted as reflecting better practice.[108] The RBA, for example, estimates that remediation for the Bank as a whole was about 93 per cent complete as at 30 September 1998 and notes that remaining *remediation effort largely relates to the provision of compliant products by third party suppliers*. It is considered that the level of confidence expressed by these bodies is supported by the governance, control and communication structures established to monitor remediation and testing activity, achieve testing objectives on time, verify

[108] Centrelink acknowledged that it had not met its own targets for the remediation and testing of some systems. However, Centrelink's targets were programmed to occur well before the Government's *Indicative Year 2000 Target Dates*, thus allowing a margin for delay.

test outcomes and, where required, implement corrective measures to mitigate the consequences of delay.

4.4 Each of these bodies is utilising a mix of strategies to address its Year 2000 problem, including retirement of redundant systems and the replacement or repair of non-compliant systems. Each body has identified core business systems which are targeted for replacement before 2000. DETYA has taken the precautionary step of rectifying systems targeted for replacement to provide a safety net against the possibility that replacement systems will not be delivered on time. The RBA, Centrelink and Customs are closely monitoring system replacement projects to enable the timely remediation of existing systems in the event that replacement is judged unlikely to occur in time.

4.5 In Customs (unlike RBA, Centrelink and DETYA) primary responsibility for the remediation, testing and assurance of IT&T systems, applications and infrastructure rests with the IT contractor under the terms of the Customs Information Technology Agreement.[109] The Year 2000 Project Team and the IT contractor meet on a fortnightly basis to discuss progress and emerging issues.[110] Although the IT contractor is responsible for the 'technical' remediation and testing of systems and applications, Customs' business units are responsible for 'business testing' to provide assurance that business processes are fully functional. Customs acknowledges that the outsourcing arrangement does not involve a transfer of responsibility for the control of business risks from the executive management to the IT service provider.

4.6 The RBA, Centrelink, DETYA and Customs have established, or are in the process of establishing, partitioned[111] test environments to support the full business testing of internal interfaces. Each body has prioritised remediation and testing activity according to assessed business importance.

[109] The IT contractor will undertake technical level remediation and testing of systems and applications. Business areas will be actively involved in testing the interfaces used to deliver business functionality. This is characterised by Customs as a 'horizontal' rather than a 'vertical' process and may in some cases involve inter-group testing. Customs points out that approximately 60 per cent of remediation work had occurred prior to the outsourcing agreement. However, this work had not been consistently documented and required further verification by the IT contractor.

[110] In March 1998, the IT contractor prepared a detailed review of Customs' Year 2000 project which included recommendations on the action Customs and the IT contractor need to take to ensure that centrally managed IT items (for which the contractor would be responsible) are Year 2000 compliant. At the same time, the IT contractor prepared a *Customs Year 2000 Project Plan* which identified the objectives, success factors, deliverables, activities, time-frames and quality assurance measures to be employed.

[111] The term 'partitioned' is used to denote a mainframe IT environment which replicates the body's business platform and enables internal interfaces between systems and applications to be tested without presenting a risk to 'live' business systems.

Responsibility for coordinating technical and business testing activity has been assigned and communicated to key business unit personnel and protocols have been established to support the verification and certification of test results and provide assurance to senior management. The RBA has estimated that as at 30 September 1998, testing is about 35 per cent complete and is scheduled for completion by end December 1998.

4.7 Each body is also liaising with key external business partners on testing issues. DETYA, for example, has established an External Assurance Testing (EAT) partition on its mainframe to allow an increased level of Year 2000 testing, including testing the inter-operability of DETYA's systems with external business partners. In general, external, or 'inter-organisational testing' should occur once internal compliance is achieved (see Figure 4.2).[112] The RBA reports that it has established a fully compliant mainframe environment and that inter-bank testing is scheduled to commence in November 1998.

DIMA, Airservices and ATO

4.8 It is essential that Commonwealth bodies closely monitor progress against their project milestones, assess potential risks to the continuity of their Year 2000 projects and prepare contingency arrangements to deal with possible delays in the renovation or replacement of critical systems.

4.9 DIMA, Airservices and ATO have each assessed the compliance status and relative business importance of their respective systems. Each has identified remediation strategies and each is relying on new systems being commissioned in time to replace existing non-compliant systems. DIMA, Airservices and ATO are confident that the remediation and internal integration testing of mission critical systems will be completed.

4.10 Airservices and DIMA have acted to remedy systemic management issues which contributed to delays with aspects of their Year 2000 projects. The consequence for both bodies is that there is less time available for remediation and testing and a much lower tolerance for project slippage. DIMA reports that progress against milestones is monitored on a monthly basis and that a risk assessment is undertaken each quarter in order to identify and manage emerging risks to the achievement of Year 2000 targets.

4.11 The ATO reported that testing would commence by mid-1998 and that all business-critical systems would be certified as compliant by 31 December 1998. Although this target is well within the boundaries of

[112] Ultimately, external testing with business partners requires that each participant first achieves internal compliance and the timing of such testing is therefore outside an individual body's control. OGO has advised the ANAO that it, in cooperation with DoFA, is currently planning a testing day, or days. OGO reports that planning is under way and involves discussions with relevant telecommunications carriers.

Figure 4.2

Inter-organisational testing and the RBA

The RBA is closely involved with the four leading Australian banks through the Interbank Working Group (IWG) which was convened in August 1997 to address common Year 2000 issues affecting the banking community, its customers and shareholders. As well as testing individual applications and carrying out inter-application testing, the RBA, through the IWG, has contributed to the development of a strategy for the testing of interbank payments streams for Year 2000 readiness. The objective of the test strategy will be to demonstrate that electronic interchanges between participating financial institutions can continue to support transactions after December 1999.

Before testing can commence, participating institutions will have to have completed internal system changes and testing and, unless otherwise exempted by the IWG, *all software applications, systems and tools, hardware components, communications networks and any other technical components, which combine to form a test environment, shall be internally or vendor certified as being Year 2000 ready.*[113] An overall Year 2000 Test Program Manager has been appointed.[114] Cross-organisational testing is due to commence in the fourth quarter of 1998 and is targeted for completion by mid 1999.

Commonwealth bodies such as Centrelink have expressed interest in participating in 'end-to-end' testing activities with the RBA and financial institutions. To facilitate this, the RBA invited Centrelink to participate in seminars convened by the IWG to discuss testing issues.[115] Although arrangements and procedures for end-to-end testing between agencies such as Centrelink, the RBA and the financial institutions have not been confirmed, it is likely that end-to-end testing would occur on a sample basis in order to demonstrate to client organisations that external interfaces will continue to function.

Source: ANAO based on information provided by the Reserve Bank of Australia.

recommended better practice, it would be advisable for ATO to strengthen aspects of its Year 2000 project governance in order to improve internal compliance with the reporting and control framework and to mitigate the risks posed by internal competition for resources.

Defence

4.12 In Defence, individual programs are responsible for the implementation of appropriate remediation strategies and testing

[113] Year 2000 Interbank Working Group (IWG), *Interbank Testing Strategy Payments Systems*, Version 2.0, 17 April 1998, p. 6. The strategy focuses on the six clearing streams associated with cheque clearing (stream 1 - APCS); direct entry (stream 2 - BECS); card schemes, EFTPOS and ATM (stream 3 - CECS); the high value clearing system (stream 4 - RTGS); the interbank paying facility (stream 5 - BPAY); and other external interfaces (stream 6).

[114] The Australian Payments Clearing Association (APCA) has appointed a contractor to coordinate the activities of Stream Test Managers. The overall Test Manager will report to the APCA Board and, through the IWG Test Group to the Interbank Working Group. The RBA will provide the Stream Test Manager for the high value clearing system (stream 4 - RTGS).

[115] On 15 July 1998, the IWG convened a seminar to outline to banks that are not members of the IWG activities of the IWG's sub-groups and its testing strategy. The seminar was also attended by the Government's Year 2000 Task Force and major telecommunications carriers gave presentations on the management of Year 2000 risks.

methodologies for business critical IT systems. At the time field work was undertaken, Defence had not developed general IT testing strategies, protocols or acceptance criteria to ensure the consistency and compatibility of IT testing activity across the portfolio. High level test strategies and systems-level test plans are being prepared for the Corporate Information Program (CIP) and Support Command Australia (SCA).[116] A contractor has been engaged to implement an overarching project management framework in CIP and will assist in the coordination of integration testing.[117] Accordingly, Defence now advises that *where the integration of IT systems is required, appropriate protocols and interface arrangements are in place or are being finalised*.

4.13 Within CIP, the Defence Computing Bureau (DCB) provides mainframe computing platforms on which Defence's core business systems reside. DCB is responsible for the coordination of integration testing of business systems across programs. Test partitions (integration testing platforms) are being established and end-to-end testing strategies and dates are being negotiated with customers.[118] The Year 2000 Project Office considers integration testing to be a priority, particularly in relation to logistic systems which are vital to maintaining mission capability. The Project Office also considers that Year 2000 priorities need to emphasise the viability of *business functions* and suggests that integration testing will help to leverage improvements in Defence's organisational and business integration generally.

4.14 Given that Defence programs' Year 2000 projects are progressing and converging at different rates, integration testing will require portfolio level coordination. It is noted that coordination of effort between programs has improved since the first quarter of 1998 and improvement appears to be continuing. A review of target dates nominated by Defence programs for the completion of remediation, testing and certification suggests that

[116] CIP and SCA together account for the majority of Defence's business critical corporate IT systems.

[117] In July 1998, KPMG Management Consulting Ltd. were engaged by Defence to carry out a scoping study to determine the range and depth of required project management for the Standard Defence Supply System (SDSS) Year 2000 project. The Scoping Study, provided to Defence in August 1998, found that the project management environment and program-level integrative processes within CIP were insufficient to integrate effort for the logistics systems domain and assure that systems provide end-to-end business outcomes. Defence subsequently engaged KPMG to provide project management resources to develop the required integrated project management capability for SDSS and associated logistics systems. Defence reports that the scope of the consultancy has been extended to cover all CIP system activities. Other contractor resources utilised by Defence include CSC (Australia), engaged in February 1998 to provide cross-program coordination of Year 2000 effort in selected enabling programs.

[118] DCB provides mainframe services to Defence under the terms of a Master Services Agreement and to Programs under Service Level Agreements.

target dates in some programs are notional and may be subject to slippage as work progresses. Delays in remediation work will result in less time being available for testing and confirmation testing.

Remediation of embedded systems

4.15 The bodies reviewed for this audit aim to assess the extent of their exposure to embedded systems by the end of the 1998 calendar year. In general, bodies will be reliant on suppliers or manufacturers to establish the Year 2000 compliance (or fitness for purpose) of embedded systems and provide solutions.[119] Bodies may own or lease the equipment affected by non-compliant embedded systems and available remedies may be contingent on conditions or limitations set out in purchase or lease agreements. In other cases, bodies may be dependent on third parties (such as building owners) to approach suppliers or manufacturers on their behalf. Awareness of embedded systems risks—particularly in relation to building services—has been slow to build. Manufacturers or suppliers may not be able, or necessarily willing to confirm the Year 2000 compliance of their products.

4.16 Taken together, these factors serve to limit Commonwealth bodies' direct control over the application and timing of remedies for business critical embedded systems. Bodies need to comprehensively map the supply chains underpinning embedded systems and assess the likely capacity of suppliers and manufacturers to supply appropriate solutions. Bodies need to have assessed the possible business, safety or legal risks posed by any failure of their embedded systems and be prepared to implement contingency arrangements.

4.17 Given that each of the eight bodies reviewed for this audit is operating within a similar time-frame with respect to embedded systems issues, the possibility exists that their experience is broadly representative of a large proportion of all Commonwealth bodies. It is also possible, that public sector progress with this dimension of the Year 2000 problem is paralleled by the private sector. This may mean that the demand for solutions to embedded systems problems will peak during 1999 with the result that key suppliers and manufacturers (some of which will be off-shore) will be unable to respond to that demand.

[119] The reference to embedded systems, in this context, is concerned primarily with building systems. The assessment and remediation of embedded systems affecting warfare assets owned by Defence is subject to more stringent testing and acceptance criteria owing to their complexity and safety-critical nature.

4.18 Finding: The ANAO found that in the Reserve Bank of Australia; the Department of Education, Training and Youth Affairs; Centrelink; the Australian Customs Service; Airservices Australia and the Australian Taxation Office:

- Year 2000 remediation is under way and quality control/quality assurance processes are being applied to the remediation process; and
- test programs have been established and some critical systems have been made either compliant or are approaching compliance.

4.19 In the Department of Immigration and Multicultural Affairs, Year 2000 remediation is under way and quality control/quality assurance processes are being applied to the IT remediation process. One major business critical system is reported to be compliant and test programs for remaining systems are in the process of being established.

4.20 In the Department of Defence, Year 2000 remediation is under way in some areas and quality control/quality assurance processes are being applied to the remediation process. Test programs have been established for systems and applications, and strategies are being prepared for the cross-program integration testing of business functions. Some critical systems are reported to have been made compliant and some have been reported as approaching compliance.

Quality assurance, certification and contingency planning

4.21 The audit examined the extent to which business critical systems and processes have been made compliant and signed off as compliant in accordance with a formal certification mechanism. The audit also examined whether bodies have commenced the development of contingency plans to ensure operational sustainability. The ANAO took into account the extent to which certification and contingency planning is governed by the following key project elements:

- mechanisms are in place to provide quality assurance about Year 2000 project activities;
- compliance certification procedures have been established to provide for executive management sign-off of compliant systems; and
- a comprehensive process has been established for the management of outstanding risks.

4.22 The ANAO considers that by mid 1998, Commonwealth bodies should be using an appropriate definition of Year 2000 compliance (see Figure 4.3). By the end of 1998, test strategies should be in place, including appropriate control structures for the validation of test results and certification of compliance; testing should be well under way for most business critical applications, systems and internal interfaces; and, strategies should be in place to manage outstanding risks and the development of Year 2000 contingency plans commenced. By mid 1999, all critical systems, critical external interfaces and most less critical systems should be compliant and certified as such by the executive management; all critical business inputs, business partners and potential supply chain risks should be identified; their Year 2000 compliance determined; and the level of residual risk comprehensively assessed; and, business continuity planning, including contingency and business resumption elements, should be substantially complete.

Figure 4.3

Definition of Year 2000 Compliance

There is a number of Year 2000 compliance definitions. The Office of Government Information Technology advocates the use of the Standards Australia definition (SAA/SNZ MP77:1998). This definition is in turn derived from the British Standards Institute definition which has been widely adopted.

The definition promoted by OGO is based on four rules of compliance:

Rule 1— No value for current date will cause any interruption in operation.

Rule 2— Date-based functionality must behave consistently for dates prior to, during and after 2000.

Rule 3— In all interfaces and data storage, the century in any date must be specified either explicitly or by unambiguous algorithms or inferencing rules.

Rule 4— Year 2000 must be recognised as a leap year in terms of handling both the 29th of February and day 366.

As the object of testing is to meet compliance requirements, testing must, as a minimum, address each rule.

Source: OGO, Year 2000 Testing Strategies, July 1998, pp. 4-5.

Quality assurance

4.23 Quality assurance can be provided in a variety of ways and may include:

- strong executive oversight through a steering committee chaired by a member of the Commonwealth body's executive management;
- the adoption by Year 2000 projects of quality processes which utilise procedures and criteria accepted as representing benchmark standards for project management;
- the ongoing monitoring and review of Commonwealth bodies' Year 2000 projects by a body's internal auditors; and
- engaging external review of aspects of a body's Year 2000 project.

4.24 In each of the bodies reviewed for this audit, executive management oversight of their Year 2000 project is provided by either a Year 2000 Steering Committee or by an executive management committee which includes Year 2000 as a standing agenda item. Of the bodies reviewed, RBA, Centrelink, DETYA, ATO and Airservices have established Year 2000 steering committees to provide oversight for their Year 2000 projects. In Customs, DIMA and Defence, Year 2000 oversight is provided by executive management committees which operate according to terms of reference which have an information technology/information management focus and address Year 2000 as a priority issue.[120]

4.25 Each of the bodies reviewed report that their Year 2000 projects have executive-management sponsorship. Centrelink and Customs reported that their Chief Executive is the Year 2000 project sponsor. In DETYA, ATO and Defence the Year 2000 project sponsor is the functional equivalent a Deputy Chief Executive[121] and in RBA, DIMA and Airservices, the Year 2000 project sponsor is the functional equivalent of a Group or Division Head[122]. In all but two of the bodies reviewed the sponsor is also a member of the Year 2000 Steering Committee or other executive management committee. In the two bodies where this is not the case, DETYA and Customs, the sponsor is briefed on Year 2000 progress by the Chair of the oversight committee in the context of an overarching executive forum.[123]

4.26 In each of the bodies reviewed, there is direct or indirect linkage between the Year 2000 project and other key Governance structures such as the body's audit committee. Each of the bodies reviewed demonstrated some level of monitoring and review by internal auditors. Internal auditors have reviewed and formally reported on bodies' Year 2000 projects in Centrelink, ATO, RBA and Defence. In DETYA and Airservices, internal auditors liaise closely with the body's Year 2000 project and provide advice in relation to due diligence and quality assurance matters. In Customs and DIMA, internal auditors maintain a watching brief on Year 2000 and have less formal liaison with their Year 2000 projects. In each of the bodies reviewed, internal auditors have expressed the intention to include Year 2000 matters as part of their future audit program. The overall Year 2000 project effort, and the quality of assurance to senior management, is greatly strengthened where internal auditors have had early pro-active involvement in the establishment of Year 2000 projects; provide ongoing

[120] In DIMA, the Alliance Group; in Defence, the Defence Executive; in Customs, the Information Technology Planning Committee.

[121] In DETYA and Defence, a Deputy Secretary; and in the ATO a Deputy Commissioner.

[122] In Airservices, a General Manager; in the RBA, an Assistant Governor; and in DIMA, a First Assistant Secretary.

[123] In DETYA, the Corporate Leadership Group; and, in Customs, the Executive Group.

advice in relation to quality assurance and due diligence issues; and undertake formal progress reviews.

Certification

4.27 Each of the bodies reviewed has established mechanisms through which accountability for key Year 2000 deliverables is communicated and confirmed with business unit managers and application/system owners. Each has implemented certification procedures and mechanisms to sign-off against the completion of their nominated Year 2000 milestones. For certification mechanisms to provide genuine assurance, bodies need to ensure that Year 2000 accountabilities are unambiguously understood and accepted and that the standards and criteria underpinning certification are robust.

4.28 These mechanisms have been effective in RBA, Centrelink, DETYA and Customs. The ANAO considers that it would be prudent to confirm business unit understanding of, and compliance with Year 2000 accountability mechanisms used in DIMA, Airservices[124], ATO[125] and Defence. All Commonwealth bodies need to ensure that business units understand and accept accountability for Year 2000 deliverables. This requires effective communication and, if left unaddressed, can create longer term impediments to the achievement of Year 2000 objectives.

4.29 Year 2000 accountability mechanisms can assist bodies to leverage a strong management focus on Year 2000 deliverables and can serve to highlight areas which require close attention. A good example is Defence which has promulgated a *Certificate of Program Year 2000 Readiness* which requires Program Heads to commit to an undertaking to ensure that certain project elements are in place and that specific outputs will be delivered within a designated time frame. Although Program Heads were required by an Executive Directive to sign a *Certificate of Program Year 2000 Readiness* by the end of July 1998, by 30 September 1998, ten out of the fourteen Defence programs had submitted signed certificates.[126] This may indicate

[124] Airservices provides example of how such confirmation might occur. In July 1998, Airservices Year 2000 Project commissioned the body's internal Quality Assurance and Certification area to review and assess business areas' compliance with Airservices' Year 2000 process and verify reports of progress. The aim of the review was to generate findings and recommendations to improve business units' compliance with reporting requirements and raise the quality of information reported.

[125] ATO advises that in 1997 the Commissioner articulated business unit accountability for Year 2000 compliance and that the ATO *has in place a detailed program to clearly articulate and assign responsibilities to those ATO officers responsible for Year 2000 compliance work.*

[126] Defence has advised the ANAO that, although CIP has not signed a Certificate of Program Year 2000 Readiness, *significant management initiatives have been implemented to effectively achieve the intent* and that *remaining outstanding certificates are delayed pending the resolution of some boundary issues.*

that program and sub-program managers in Defence are still assessing their ability to achieve their Year 2000 objectives.

Contingency planning

4.30 None of the Commonwealth bodies reviewed has yet developed Year 2000 contingency, emergency response or resumption plans. All of the bodies reviewed have existing disaster recovery strategies for particular systems or applications and most will have business resumption strategies for particular service delivery elements. Bodies such a Centrelink and RBA, for example, have strategies in place to provide fall-back options or 'work-arounds' which will allow business to carry on, perhaps at a reduced level, in the event of technology failure or natural disaster. Airservices and Defence have multiple-level contingency arrangements, particularly in business areas exercising safety critical functions. There is no certainty, however, about the ability of existing contingency arrangements to deal with all possible Year 2000 failure scenarios.

4.31 Year 2000 contingency planning has begun, albeit tentatively, in most of the bodies reviewed. All of the bodies reviewed consider that contingency planning will be most effective if undertaken in late 1998 through early 1999 once the results of their, and their business partners', initial testing are available. It is contended that this will allow bodies to more accurately identify likely residual risks and focus attention on strategies for specific risk scenarios. Most bodies are aiming to complete contingency planning activity before the end of 1998.

4.32 Two bodies, DETYA and Airservices, have sought external assistance with Year 2000 contingency planning activity. DETYA has invited tenders for a consultancy to address Year 2000 risks to business continuity.[127] In June 1998, Airservices invited tenders for the development of Year 2000 Business Risk Management Plan which will provide a basis for Year 2000 contingency planning which will complement existing contingency arrangements.

4.33 Customs and ATO are preparing contingency planning guidelines to be used by business areas and Centrelink is preparing a whole-of-business continuity strategy which will provide a platform for the development of Year 2000 contingency plans by business units. The RBA is currently reviewing its existing disaster recovery and business

[127] In June 1998, the then DEETYA invited tenders for the preparation of a Continuity Management Plan which was to take account of general and Year 2000 risks to business continuity. Subsequently, DEETYA decided not to proceed with a combined tender and has moved to invite a separate tender for work in relation to Year 2000 business continuity risks.

resumption plans and business units are expected to incorporate contingency planning strategies at each phase of their Year 2000 activity.

4.34 DIMA is aiming to complete Year 2000 contingency plans by September 1999. Although DIMA will have completed its assessment of its internal Year 2000 exposures before the end of 1998, the full results of testing are not likely to be available until the first quarter of 1999.

4.35 In preparing its contingency plan(s) DIMA will need to be mindful of its extensive off-shore presence. Although other selected bodies, such as RBA, Customs and Defence, have personnel and premises overseas, these are predominantly located in developed industrialised nations which are at the forefront of Year 2000 preparedness. DIMA, by contrast, has personnel stationed in countries which may not be well prepared for the Year 2000 and may be at risk of economic dislocation and social unrest during the change-over period. DIMA will, therefore, need to give careful consideration to the protection of personnel in high risk locations in partnership with other relevant agencies.[128]

4.36 Defence has not yet initiated a coordinated approach to contingency planning, although a number of contingency-related activities are under way across the portfolio. Defence programs support the concept of portfolio wide coordination of Year 2000 contingency planning and the Year 2000 Project Office recognises the need to harmonise the priorities and contingency arrangements across programs. Defence has commented that *contingency planning needs to be considered in the knowledge of the risks and it is not cost effective to implement early contingency planning when the circumstances do not justify*. Defence has advised the ANAO that many Defence activities are, in the normal course of events, supported by contingency planning processes and that the inclusion of Year 2000 aspects will occur as risks are clarified through ongoing analysis. Nevertheless, the uncertainties, lack of relevant expertise and resource shortages would suggest that a prudential approach be taken to the consideration of contingency arrangements, particularly in view of the potential impacts on outputs and outcomes.

[128] The Department of Foreign Affairs and Trade (DFAT) portfolio has initiated a three tiered approach to the assessment and management of extra-territorial Year 2000 risks. The first tier is examining the compliance of overseas posts and the risks associated with the potential interruption of essential services; the second involves research in relation to the extent of Year 2000 risks in countries in which posts are located; and, the third involves an examination of issues pertaining to the safety of overseas personnel and a study of potential Year 2000 economic risks in the Australasian region. DFAT has informed the ANAO of its intention to contact other Commonwealth agencies with personnel posted overseas to apprise them of these initiatives.

4.37 As it is possible that remediation and testing activity for some major Defence systems will occur at the extreme limits of acceptable time frames, the need to develop contingency plans is accentuated.[129] For example, because Year 2000 failures are likely to occur in the Australian summer when there is an increased risk of severe tropical storms and bush fires, Defence will need to ensure a continued capability to deliver civil aid in the event of a natural disaster.

4.38 **Findings:** The ANAO found that in the Reserve Bank of Australia; the Department of Education, Training and Youth Affairs; and Centrelink the development of contingency, business continuity and/or business resumption plans for the management of residual Year 2000 risk has commenced, although the nominated time frames for completion vary.

4.39 In the Australian Customs Service and the Australian Taxation Office the development of contingency, business continuity and/or business resumption plans has not commenced, although contingency planning guidelines are being developed.

4.40 In Airservices Australia and the Department of Immigration and Multicultural Affairs the development of contingency, business continuity and/or business resumption plans to address Year 2000 specific risks has not commenced. Airservices has indicated that existing contingency arrangements would be updated to take Year 2000 issues into account during 1998. DIMA intends to complete Year 2000 contingency planning by September 1999.

4.41 In the Department of Defence the development of Year 2000 contingency, business continuity and/or business resumption plans has not commenced in most programs and an indicative time-table for a portfolio-wide contingency plan has not been established. It is noted that some Defence activities are currently supported by contingency planning processes although these may not address all risks arising from Year 2000 related events.

Recommendation No. 4

4.42 ANAO recommends that Commonwealth bodies that have not already done so, give urgent attention to the development of contingency plans, including emergency response and resumption plans, which address Year 2000 within an overall continuity management approach.

[129] There is a recognition that capability programs may need to utilise ‘work-around’ options in the event of mission critical systems not being available.

4.43 Selected Commonwealth bodies responded to the recommendation as follows:

- ***Agree:*** Airservices, ATO, Centrelink, Customs, Defence, DETYA, DIMA and RBA.

4.44 Specific Comments by selected Commonwealth bodies are set out below:

- ***RBA response:*** RBA advises that, internally, the Bank is currently augmenting its existing business continuity plans by identifying and assessing likely Year 2000 risks and responses which would impact our overall business delivery. Externally, the Bank is participating in the Interbank Working Group (IWG) Risk Management sub-group which has released the document *'Year 2000 Risk Management and Contingency Planning Framework - Institutional Level'*. The Bank is also participating in the APCA Continuity Planning Consultative Committee which is looking at continuity issues relating to the Australian Clearing Streams.
- ***Airservices response:*** Airservices advises that it has already commenced analysis of critical processes and undertaken a series of technical design reviews to assess the robustness and recovery options for some of its major systems. This will form a basis for the specific Y2K contingency plans. Airservices acknowledges that contingency planning will take more time than originally estimated, and in order to be consistent with the timetable of major partners will not be completed by the end of 1998 as originally planned. Additional resources have been allocated to this task.

5. Managing change past the turn of the century

This chapter examines selected Commonwealth bodies' management of Year 2000 project risks associated with organisational change processes and considers what selected Commonwealth bodies need to achieve between now and 2000.

Change management

5.1 An organisation's Year 2000 project is, in many respects, a change management initiative. Although the essence of a Year 2000 project is prevention, this may entail aspects of re-engineering, process re-design, the replacement or retirement of business systems, extensive internal and external communication efforts and the promotion of adaptive behaviours. In organisations which do not have a strong record of effective change management, Year 2000 initiatives may be subject to high levels of project risk.

5.2 There is minimal scope for slippage in the achievement of an organisation's Year 2000 milestones. The end-date for achieving compliance cannot be moved and organisations need to allow sufficient time for testing and rectification of outstanding problems. The simultaneous management of major projects which place competing demands on a limited pool of financial, human and technical resources can result in delay or may compromise the achievement of targets. The Government has acknowledged that because Commonwealth bodies are required, for the most part, to meet remediation costs from within their existing budgets, *this may mean* [that] *scheduled new projects or other applications development must be put on hold until this problem is corrected.*[130]

5.3 Public sector organisations are particularly susceptible to change. In the time remaining until 2000 a number of Commonwealth bodies will experience a re-structure, re-organisation or re-profiling of their business as a result of government policy and changes in market conditions. Organisations with demonstrated strengths in change management may even use their Year 2000 projects to leverage a stronger competitive position through improved service delivery and enhanced customer loyalty. It will be essential for bodies to manage the change process in such a way as to not compromise the achievement of their Year 2000 objectives. DIMA, for

[130] Minister for Finance and Administration, *Millennium Bug: Government Readiness*, Media Release (38/98), 24 April 1998.

example, includes Year 2000 impact statements in all submissions and new policy proposals.

5.4 Each of the selected bodies have undergone, or will undergo major organisational changes. In particular, Centrelink, DETYA and Defence have been required to re-engineer business processes, either to give effect to new policy initiatives of Government, or as part of efforts to renovate aspects of their business systems.

Centrelink

5.5 As a relatively new organisation, Centrelink has been required to address its Year 2000 problem whilst at the same time creating and consolidating its management structure and business operations. The period from Centrelink's inception to the present has been one of intensive change and has involved the implementation of a new business culture, systems and processes.

5.6 Centrelink is working to ensure that its business operates on a sound commercial footing. In recognition of recent trends towards the introduction of greater contestability into the procurement and delivery of Government mandated services, Centrelink is working towards the goal of delivering services at a competitive price by 2000. Centrelink is also conscious of the need to establish and reinforce customer loyalty to ensure its long term commercial viability. Centrelink recognises that its longer term viability could be strengthened through the diversification of its business mix (both clients and products). In order to reduce its commercial exposure to its larger clients, Centrelink is actively growing its business by tendering for contracts with a wider range of organisations, including State and local governments.[131]

5.7 Centrelink's business processes are highly dependent on technology and the organisation's dependency on IT and telecommunications is rapidly increasing with the take up of call centre technologies and electronic commerce. Centrelink recognises the opportunity to use its systems and management, which includes the management of its Year 2000 problem, as a commercial lever to win customer loyalty and to enhance its competitive position as a provider of electronic financial or case management services.

5.8 As with any other business, it should be recognised that Year 2000 will impose a net cost on Centrelink's operations which will not deliver an off-setting return on investment. However, as many businesses are realising (and as the Government's Year 2000 Task Force has emphasised) Year 2000

[131] At present, the majority of Centrelink's business derives from the Department of Social Security, DEETYA, DEWRSB and the Department of Health and Family Services.

preparedness not only ensures business continuity, but may also confer a competitive advantage. As Centrelink grows its business, it will need to be cognisant of the potential to alter its current risk environment. Centrelink senior management recognises the potential to introduce new Year 2000 problems through the re-engineering of existing systems to accommodate new business lines, or the installation of new systems to provide services to clients. Controlling these risks will require close monitoring to 2000 and beyond.

DEETYA

5.9 During 1996-97 and 1997-98, the former DEETYA was required to manage the implementation of major change processes associated with employment services reforms and market testing information technology infrastructure maintenance. The reforms implemented by DEETYA involved the establishment of a competitive employment services market[132] and the transfer of public contact services from the former Commonwealth Employment Service to Centrelink. This required substantial changes to existing business processes and associated information technology.

5.10 The restructuring of employment services has entailed the replacement of core business applications as well as the development and commissioning of new business systems. Coupled with the market testing exercise for IT infrastructure maintenance, there was significant potential internal competition for the same human, financial, technical and management resources required for the then DEETYA's Year 2000 effort. In addition, each of these initiatives was subject to intractable deadlines and could not tolerate slippage. The simultaneous management of the three initiatives set a significant management challenge and potentially accentuated the organisation's Year 2000 risks.

5.11 The former DEETYA appeared to have recognised the opportunities to realise the potential synergies. For example, the implementation of new employment services required the re-engineering of some core business processes which, in turn allowed the organisation to replace or upgrade business systems with Year 2000 compliant products. In addition, the IT market testing initiative provided additional incentive to establish a complete and accurate IT inventory. Administrative changes announced by the Government in October 1998, have resulted in the transfer of employment services to the new Department of Employment, Workplace Relations and Small Business (DEWRSB). A coordinated approach will be

[132] Achieved through the creation of Employment National from 1 May 1998 - a corporatised public provider assuming most of the responsibilities formerly exercised by the Commonwealth Employment Service (CES) - and the use of contractual arrangements to purchase employment services from non-government providers.

required in order to effect the transfer while ensuring the continuity of Year 2000 activities for associated business systems.

Defence

5.12 The Defence Reform Program (DRP) provides an example of the potential risks to the continuity of a Year 2000 project posed by major organisational re-alignments. The DRP grew out of the Defence Efficiency Review, established in October 1996 to examine Defence management, eliminate unnecessary administrative practices and duplication, and to ensure that Defence focused on core functions. The DRP involved a major re-organisation of the Department, including a move from an eight program to a more functionally based 14 program structure (from 1 July 1997). The DRP also involved civilian and military staff reductions, the co-location and reorganisation of acquisition functions, the consolidation and rationalisation of support and administrative functions and the establishment of new program and sub-program elements.[133]

5.13 The DRP has been cited within Defence as a contributor to the Department's slow progress with its overall Year 2000 effort. Although it is not possible to quantify the overall impact on Defence's Year 2000 effort, discussions with Defence personnel indicate that the implementation of the DRP has caused uncertainty, dislocation and confusion and this has served to delay Year 2000 work by siphoning resources, supplanting priorities or impairing cooperation. These issues are generally recognised and are being progressively resolved.

5.14 Conversely, the DRP has provided a more rational and coherent environment in which to address the Year 2000 issue and the Year 2000 issue has, in some respects, been a driver for the consolidation of change. The Defence Year 2000 project has also observed that the co-location of previously dispersed functions within a rationalised organisational structure has made the coordination of Year 2000 activity much easier than it would have been under the previous structure.

5.15 **Finding:** Each of the selected Commonwealth bodies has recently experienced, or will undergo, some degree of organisational change. In particular, Centrelink, the Department of Defence and the Department of Education, Training and Youth Affairs have been required to manage their Year 2000 Projects in the midst of major corporate change processes.

5.16 Each of the selected bodies recognises the risk that Year 2000 projects may be adversely affected by competing demands on executive management attention and resource competition in a change environment.

[133] Department of Defence, Annual Report 1996-1997, p. 12.

Selected bodies acknowledge the potentially heightened risk to the continuity of Year 2000 effort as a result of implementing changes to business critical systems, particularly during the latter half of 1999. Selected bodies also recognise the opportunities presented in a change environment to rationalise, renovate and/or replace business systems and, thereby, reduce their Year 2000 exposures.

5.17 By comparison with other selected bodies, the magnitude of organisational change in Defence has imposed significantly greater demands and presented greater challenges to its overall Year 2000 efforts. Although the implementation of the Defence Reform Program has provided opportunities to leverage positive Year 2000 outcomes, it has also entailed opportunity costs as a consequence of a degree of dislocation and uncertainty which has accompanied major organisational changes. The situation has shown significant improvement and the Defence Year 2000 Project Office is working to reduce the risks and realise the benefits presented by this major change process.

Recommendation No. 5

5.18 ANAO recommends that Commonwealth bodies incorporate Year 2000 impact statements within all proposals or submissions leading to the implementation of major organisational or business changes.

5.19 Selected Commonwealth bodies responded to the recommendation as follows:

- ***Agree:*** Airservices, ATO, Centrelink, Customs, Defence, DETYA, DIMA and RBA.

5.20 Specific Comments by selected Commonwealth bodies are set out below:

- ***RBA response:*** RBA advises that the Bank currently considers the likely impact of Year 2000 in any major organisational or business change.
- ***Airservices response:*** Airservices advises that since the audit, the organisation has undergone an internal restructure. The Year 2000 project office has confirmed existing, and established new, links with the new management structure and expects that the new arrangements will be satisfactory. To retain the high profile of Year 2000, the Project Manager reports to the Director of Operations Support who is a member of the Airservices Australia Executive. This was identified in the impact statement prepared in relation to the changes.

Selected bodies' future Year 2000 progress

5.21 In the course of this audit the ANAO has observed the presence in each of the selected bodies of corporate governance structures, control systems and project management arrangements established to address the Year 2000 problem. In general, the bodies reviewed for this audit exhibit a good understanding and an appropriate sense of urgency about Year 2000 issues. Although the eight bodies reviewed are not representative of the wider Australian Public Service (in particular, their circumstances are not representative of those facing smaller bodies) they are, nevertheless diverse in terms of the nature of their business, their operating environments and the mix of technology and other business inputs on which they depend. The size and nature of their Year 2000 task differs and their respective Year 2000 projects have been subject to differing opportunities and constraints. Even so, these bodies have many issues in common and a number even have converging interests. A shared priority for each of the selected bodies is to ensure that their business functions continue to operate over the turn of the century.

5.22 The ANAO considers that, by the end of the 1998 calendar year:

- comprehensive inventories of IT and non-IT business elements should be well established and subject to robust control processes to ensure their continuing accuracy;
- business impact assessment should be completed and robust mechanisms established to ensure that the assessment is able to be revised in accordance with dynamic project priorities based on ongoing risk assessment and quality assurance;
- remediation should be complete for all critical systems with less critical systems being addressed subject to equivalent quality standards;
- test strategies should be in place, including appropriate control structures for the validation of test results and certification of compliance;
- testing should be well under way for most business critical applications, systems and internal interfaces; and
- strategies should be in place to manage outstanding risks and the development of Year 2000 contingency plans commenced.

5.23 The ANAO considers that, by mid-1999:

- all critical systems, critical external interfaces and most less critical systems should be compliant and certified as such by the executive management;

- all critical business inputs, business partners and potential supply chain risks should be identified; their Year 2000 compliance determined; and the level of residual risk comprehensively assessed; and
- business continuity planning, including contingency and business resumption elements, should be substantially complete.

5.24 The ANAO notes that a number of selected bodies have deferred the remediation of non-business critical systems and applications and recognises that remediation activity will continue into 2000. Bodies with significant external dependencies and large volume transactions may need to consider the implementation of audit programs in order to reconcile receipts and/or expenditures against historical data or modelled performance in order to ensure the correct functioning of business processes.

5.25 Defence acknowledges that compliance will not be achieved for all systems and is therefore focusing its efforts on those core systems necessary to ensure mission capability. Defence advises that all *available analysis confirms a high probability of compliance being achieved* for core systems and comments that *any other outcome is unacceptable*. Defence has taken steps to accelerate and better coordinate its overall Year 2000 effort. The effectiveness of these measures will need to be closely monitored.

5.26 **Findings:** Selected Commonwealth bodies have established, as of September 1998, Year 2000 project management systems and structures necessary to effectively manage their Year 2000 risks and achieve outstanding targets provided they maintain their current level of effort and there is no marked change in their operating environments. After the turn of the century, all Commonwealth bodies will have to validate the performance of critical systems as well as continue the remediation and testing of non-critical systems. However, major organisational changes and/or the implementation of new business systems to support new policy initiatives could affect the progress of Commonwealth bodies' Year 2000 projects.

Recommendation No. 6

5.27 ANAO recommends that Commonwealth bodies:

(a) comprehensively review their progress to date; assess the Year 2000 targets and milestones which must be achieved in the time remaining; and identify potential risks to the achievement of compliance for business critical systems and functions;

(b) identify activities to be undertaken to renovate, replace or retire remaining systems; guard against re-occurrence; and audit the post-2000 performance of business processes to ensure correct functioning; and

(c) prepare a Year 2000 transition plan, using a documented process for accountability and awareness-raising purposes, to manage the migration of dedicated Year 2000 resources and control structures to a 'business-as-usual' environment during the calendar Year 2000.

5.28 Selected Commonwealth bodies responded to the recommendation as follows:

- ***Agree:*** Airservices, ATO, Centrelink, Customs, Defence, DETYA, DIMA and RBA.

5.29 Specific Comments by selected Commonwealth bodies are set out below:

- ***RBA response:*** In relation to recommendation 6(a), RBA advises that status reports covering these issues are provided approximately every six weeks to the Bank's Year 2000 Steering Committee.
- ***Airservices response:*** Airservices advises that its Year 2000 Project Contingency Plan includes requirements for ongoing reviews, transition arrangements for Year 2000 events, and a post-2000 performance appraisal.

Canberra ACT
15 December 1988

P. J. Barrett
Auditor-General

Appendices

Index

Series Titles

Titles published during the financial year 1998-99

Audit Report No.1 Performance Audit
Corporate Governance Framework
Australian Electoral Commission

Audit Report No.2 Performance Audit
Commercial Support Program
Department of Defence

Audit Report No.3 Performance Audit - Follow-up
Assessable Government Industry Assistance
Australian Taxation Office

Audit Report No.4 Performance Audit
Client Service Initiatives
Australian Trade Commission

Audit Report No.5 Performance Audit
Commonwealth Agencies' Security Preparations for the Sydney 2000 Olympics

Audit Report No.6 Audit Activity Report
Audit Activity Report: January to June 1998
Summary of Outcomes

Audit Report No.7 Performance Audit
Management of the Implementation of the New Employment Services Market
Department of Employment, Education, Training, and Youth Affairs

Audit Report No.8 Performance Audit
Safeguarding Our National Collections

Audit Report No.9 Performance Audit
Accountability and Performance Information
Australian Sports Commission

Audit Report No.10 Performance Audit
Sale of One-third of Telstra

Audit Report No.11 Performance Audit
OGIT and FedLink Infrastructure
Office of Government Information Technology

Audit Report No.12 Performance Audit
Taxation Reform
Community Education and Information Programme

Audit Report No.13 Performance Audit
Aboriginal and Torres Strait Islander Health Program
Department of Health and Aged Care

Audit Report No.14 Performance Audit
Prescribed Payments Scheme
Australian Taxation Office

Audit Report No.15 Performance Audit
Postal Operations
Australian Customs Service

Audit Report No.16 Performance Audit
Aviation Security in Australia
Department of Transport and Regional Services

Audit Report No.17 Performance Audit
Acquisition of Aerospace Simulators
Department of Defence

Audit Report No.18 Performance Audit
Accounting for Aid — The Management of Funding to Non-Government Organisations — Follow Up Audit
Australian Agency for International Development (AusAID)

Audit Report No.19 Performance Audit
The Planning of Aged Care
Department of Health and Aged Care

Audit Report No.20 Financial Statement Audit
Audits of the Financial Statements of Commonwealth Entities for the Period Ended 30 June 1998
Summary of Results and Financial Outcomes

Audit Report No.21 Financial Control and Administration Audit
Costing of Services

Better Practice Guides

Asset Management	Jun 1996
Paying Accounts	Nov 1996
Audit Committees	Jul 1997
Public Sector Travel	Dec 1997
Controlling Performance and Outcomes	Dec 1997
Protective Security Principles (in Audit Report No.21 1997-98)	
Management of Accounts Receivable	Dec 1997
AMODEL Illustrative Financial Statements 1998	Jul 1998
New Directions in Internal Audit	Jul 1998
Security and Control for SAP R/3	Oct 1998