The Members of the Legislative Assembly
Parliament House
SYDNEY NSW 2000

In compliance with Section 38E of the *Public Finance and Audit Act 1983,* I present a report to the Legislative Assembly titled **1999 - 2000 Millennium Date Rollover.**

A C HARRIS

Sydney
December 1997

Performance Audit Report

**1999 - 2000
Millennium Date Rollover**

- **Preparedness of the NSW
  Public Sector**

Table of Contents

Executive Summary

Executive Summary

The Year 2000 problem, known as the "Y2K" problem, has occurred because of the use, storage and manipulation of a two digit century/year code rather than a four digit century/year date code in product applications. Two digits were used by programmers because this method was convenient and saved on memory.

If not corrected, the use and manipulation of affected products will lead to incorrect calculations and malfunctioning of time based control systems. That is, it will affect all automated information processing equipment and instructions including:

- computer hardware and computerised devices

- computer firmware (application software embedded into a computer)

- computer applications (purchased software applications, computer systems software and data).

Overall, The Audit Office found that the NSW public sector is not as prepared as it could be. Beginning in May 1996, the Department of Public Works and Services (DPWS) commenced a program to increase awareness of, report on and assist agencies with Year 2000 issues. However, significant areas of risk are still yet to be fully assessed, and action to resolve and implement appropriate solutions are lagging in areas of the public sector. A substantial acceleration and expansion of Year 2000 related activity is essential over the next twelve months to address this situation.

In broad terms, the Year 2000 problem could affect both information technology (IT) and non IT. The latter includes systems dependent upon programmable logic controllers. These drive machines and equipment, including building services and medical equipment.

In the public sector, revenue collection systems, records systems, waiting lists and payment systems are examples of business processes which could be affected.

This performance audit was undertaken to identify and evaluate the risks and costs to the NSW public sector of the Year 2000 problem and the likely costs of rectification.

In detail, the audit found that:

- some IT and non IT areas of particular vulnerability or exposure to the Year 2000 bug can be identified

- other risks cannot be identified precisely because the degree of risk depends on:

    - the compliance of services and products provided by customers and suppliers (the supply chain)

    - interfaces (exchange of data needs to be managed)

- therefore, the nature and extent of full risks and total costs to the State cannot be identified

- factors which affect Year 2000 exposure for public sector agencies include:

    - the nature of the business

    - organisational characteristics such as a decentralised or centralised structure

    - the nature, size and complexity of the IT environments used

    - whether information critical to the business is contained on a system maintained by the business

    - the nature of date-based control/access non IT and telecommunications used (affecting building services and medical equipment)

    - the nature and extent of reliance on suppliers and other agencies in data exchange and supply of products and services

    - whether resources (staff, finance and equipment) are available to resolve any problems.

The audit found that the major problems facing agencies are:

- lack of awareness of issue

- lack of a business risk culture which would recognise Y2K as a business issue

- nature of the organisational structure

- the need for asset management that is appropriate for the nature of IT, business and equipment environments

- need for recognition of agency dependencies

- need for project management across the agency

- difficulties in defining resolution costs.

The major problems facing the NSW public sector as a whole are the need for:

- a more precise identification of State wide risks. This should include those agencies and functions which pose high risks

- central agency facilitation of DPWS' strategies designed to implement the Government's endorsed Year 2000 policy. This would increase the effectiveness and efficiency of their efforts

- development of a consistent definition for Year 2000 across the public sector

- assessment and resolution of legal matters at an agency and whole of Government level. Particular attention should be given to any risks posed if regulatory agencies fail to alert businesses of Y2K problems

- management of Year 2000 through purchases (tenders) and contracts

- consideration and resolution of financial issues.

The Audit Office of New South Wales will be investigating the impact Year 2000 would have for the financial audits of agencies. It will also evaluate the implications of Y2K impact for The Audit Office opinion that is expressed in the financial statements.

The audit commenced in September 1996.

Recommendations

1. To reduce risks and costs within relevant agencies, it is recommended that they:

    - develop an internal Y2K awareness campaign for all staff

    - recognise Y2K as a business issue

    - treat Y2K as a risk management exercise

    - utilise a project management approach such as the one developed by DPWS to identify, assess and address risks.

2. To reduce risks and costs to NSW and the NSW public sector, it is recommended that the NSW Government:

    - activate a central agencies program[1] which would provide DPWS' Government Information Management Board (GIMB) with expert advice and assistance (see Attachment 2)

    - adopt an adequate and consistent definition of Y2K compliance to be used in all IT and non IT tenders, contracts and purchasing arrangements

    - through DPWS maintain a strategic approach to Y2K issues. The approach should include targeting high risk agencies and functions and minimising duplication of agency effort in addressing Y2K problems.

3. To provide accountability to the NSW public, it is recommended the NSW Government report on the effectiveness of Y2K strategies by:

    - requiring agencies to publish their risk management activities for the Y2K problem in their Annual Report

    - providing a publicly available, consolidated Y2K report prepared by central agencies which includes information on IT and non IT areas and agencies and functions at risk.

---

[1] The central agencies program was originally proposed by DPWS and endorsed by the NSW Government.

Response from the Director-General, Department of Public Works and Services

Thank you for the opportunity to respond to the Performance Audit Report *1999-2000 Millennium Date Rollover"* prepared by The Audit Office. As you are aware, the Department of Public Works and Services (DPWS) worked closely with The Audit Office in the development of the Report.

As indicated in the Performance Audit Report, DPWS actively commenced addressing the Year 2000 problem on a whole-of-Government basis early in 1996. As the result of those early activities, it became apparent that the extent of the problem and the general unpreparedness of agencies was a cause for major concern. Accordingly, strategies to improve the management of the Year 2000 problems were prepared for Cabinet and endorsed in June 1997.

Following Cabinet endorsement, a whole-of-Government Year 2000 project team of three people was established within DPWS with recruitment finalised by September 1997. Since then, a significant number of activities, many of which have been referred to in your report, have been undertaken to increase the awareness not only of government agencies, but also local government and the private sector.

I would endorse the major thrust of the report with its identification of the Year 2000 problem as both a business issue and a risk management activity. It has been our experience to date, that far too many organisations, both private and public, still consider this to be purely an information technology problem Nothing could be further from the truth and DPWS will contribute much of its effort to changing this erroneous perception.

With the Year 2000 business risk analysis methodology now in place, DPWS is actively working with agencies in the application of that process. Coupled with the establishment of the panel contract of Year 2000 business analysts, agencies will be required to submit their Year 2000 strategies for assessment by the Government Information Management Board.

Risk management software has been acquired by the project team and agency Year 2000 strategies and activity will be captured by DPWS to provide a whole-of-Government perspective for regular reporting to Government.

The Government Information Management Board, with its whole-of-Government focus and representation from the central agencies, has been actively involved in monitoring Year 2000 progress. The Board now intends to require significantly more Year 2000 accountability from agencies and will seek the participation of both the Attorney-General's Department and The Audit Office in that activity.

Finally, a number of other initiatives are well underway. To complement the methodology, a cut down eight page version is being developed for use by smaller organisations including local government, small to medium enterprises and the general community. Copies of this document will be provided both on the Government Year 2000 Internet web site as well as being mailed out through the Department of Fair Trading and State and Regional Development.

A panel contract for the establishment of Year 2000 remedial service for a variety of activities is currently a tender and is expected to be in place by mid December. Year 2000 compliance definitions have been developed in conjunction with the Crown Solicitor's Office and is now being included in all tender documents. A Year 2000 product compliance warranty has also been prepared. Familiarisation seminars for both the public and private sectors are an ongoing activity and it is pleasing to note that these seem to be gradually raising the required level of awareness.

Finally, let me say that I am very pleased with the cooperation between The Audit Office and DPWS in the development and finalisation of the Report. DPWS does not underestimate the challenge offered by the millennium bug and our aim is to excel in the outcomes for the NSW Government by minimising the risks posed to the operation of Government from this 1999-2000 millennium date rollover.

(signed)

Dick Persson
Director-General

1. Introduction

1.1   Introduction

This chapter defines the nature and scope of the Year 2000 problem and evaluates how it might affect the NSW public sector.

The Year 2000 problem, colloquially known as "Y2K" or the "Millennium Bug" arises because of the use, storage and manipulation of a two digit century/year date code rather than a four digit century/year date code in product applications. Two digits were used by programmers (throughout the 1960s up until the mid 1990s) because memory was expensive and it was convenient at the time.[2]

Programs which sort information according to date or which perform computations on date elements may not act the way one would expect them to work.[3] Calculations (that pre-suppose a leading century prefix eg 19XX) will be incorrect. Time based access control systems (that also pre-suppose a leading century prefix eg 19XX) will be affected.

The Year 2000 problem will affect all automated information processing equipment and instructions where a computer processor incorrectly stores and uses dates in calculations or date-based access facilities. These could include:

- computer hardware and computerised devices
- computer firmware (application software embedded into a computer)
- computer applications (purchased software applications, computer systems software and data).

Some consider that the risks created by the Year 2000 will be massive and costs of rectification extremely high. Such a view can be seen in the literature and in initiatives taken by some jurisdictions. It can also be seen in speeches by Government Ministers. The Hon Carl Scully, Minister for Public Works and Services and Assistant Minister for State and Regional Development indicated that lack of attention to the Year 2000 problem could have "dire consequences" and that rectification costs for New South Wales (NSW) as a whole (public and private sectors) could be as high as \$4 billion.[4] The issue had earlier been raised in the NSW Parliament.[5]

---

[2] The problem is compounded by the fact that some programs use the digits 99 as a control method to mark the end of files. This means that in 1999, errors and failures of systems could occur.

[3] USA National Institute of Standards and Technology (NIST).

[4] DPWS Summit Year 2000 24 July 1997 and interview with Minister Scully, Business Review Weekly (BRW), 19 May 1997, p. 49.

[5] Legislative Council 17 October 1996.

Given the possible widespread risk, this audit was initiated in September 1996 to "identify and evaluate the risks to the NSW public sector of the Year 2000 problem and the likely costs of rectification". The criteria for the audit are at Attachment 1.

1.2   What will be Affected?

An agency could experience Year 2000 problems in its environment, external business links and internal systems (see Diagram 1).

To determine whether a problem exists, it is crucial to seek a manufacturer's statement regarding Year 2000 compliancy status of that particular model of equipment or release of software.

Rules/Criteria for Compliance

Essentially, while there are different definitions of Year 2000 compliance or conformity, it means that "neither performance nor functionality is affected by dates prior to, during and after the year 2000."[6] The rules for compliance/conformity are:

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 Year 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.[7]

The DPWS emphasise that while individual software may comply with these criteria, other factors such as the customisation of software or its use in conjunction with other software products, may render it not compliant.

---

6 DISC, British Standards Institution, 18 June 1997 Internet page, p. 1.
7 ibid, p. 1.

Diagram 1: Year 2000 Date Change Impact Relationship Model [8]		
Business Domain		
Information Technology Domain		
Agency Environment	**External Business Links**	**Internal Systems**
air conditioning systems	contracted out services (payroll, HR etc)	hardware
security/surveillance systems	suppliers of goods, essential to program management	operating systems software
control panels	goods, services or information provided to customers	interconnections and bridges
scientific measuring equipment		screen displays and printed and other outputs
lifts		end-user applications (spreadsheets, databases)
PABX		forms, stationary, contracts etc
any equipment with an embedded chip hardware		

Organisations such as Telstra have developed criteria against which they will measure applications to evaluate if the application is fully Year 2000 compliant. Telstra have six such criteria:

- *integrity* - accepts and correctly processes valid dates and times in both the 20th and the 21st century

- *discrimination* - ensures that within an application, dates in the 21st century are unambiguously distinguishable from dates in the 20th century to allow correct processing across the millennium change

- *process* - continues to produce correct results before, during and after the date changes from 31 December 1999 to 1 January 2000, irrespective of whether or not it is operating at the time the change occurs

- *order* - in all respects, treats the year 2000 as the year that immediately follows the year 1999, and the year 1999 as the year that immediately precedes the year 2000

- *calculation* - performs all date and time calculations and comparisons correctly, regardless of the mixture of 20th and 21st century dates and times involved

- *leap year* - recognises that the year 2000 is a leap year.[9]

---

[8] WA "Year 2000 Date Change" Policy Statement.

[9] These compliance criteria are an extract from Telstra's Policy Document 006 494 - IT Year 2000 Compliance - which is for internal use, for Telstra's computer applications. It is reproduced here with Telstra's permission.

**Vendors'
Compliance**

Suppliers have indicated a range of responses to DPWS' query as to whether the Year 2000 poses a compliance problem for the operation of their software or firmware products.   These responses, inferring different risks, include:

- there is no compliance problem

- the issue is currently being investigated

- the problem will be overcome in an upgrade.

Supply complications include:

- vendors of previously purchased products may no longer be in business

- some vendors choosing to close and not to rectify a Year 2000 problem.   This may be an alternative to accepting of responsibility for fault correction

- vendors relying on compliance assurances by third party suppliers.

1.3   Risk to the Public Sector

Risk refers to "the chance of something happening that will have an impact on objectives. It is measured in terms of consequence and likelihood".[10]   Generic sources of risk relevant to the Year 2000 issue include:

- technology and technical issues

- commercial and legal relationships

- economic circumstances (availability of funds to fix the problem)

- management activities and controls

- individual activities (responsibility for fixing problem).

If systems fail, the **consequences** (or impact) in the public sector can be direct or indirect. Possible direct consequences include:

- failure in the provision of critical services such as health and transport

- threats to personal safety eg if medical equipment fails

- inability to collect vital revenue to fund services.

---

[10] AS/NZS 4360:1995 cited by EDS, 1997, p.1.

Indirect impacts include legal risks, failure in statutory financial requirements, increased staff workload and the need to address contract design management issues.

In order to evaluate the consequences of not addressing the Year 2000 problem, it will be important to identify which business processes rely on date-based calculations (mostly confined to IT&T products). Similarly, it will be essential to distinguish which services are dependent on date-based access/control systems (mainly confined to non-IT and telecommunications equipment) and which services are not.[11]

Consequence of Date-based Calculations

There is potential for the Year 2000 problem to affect calculations relating to issues such as staffing matters (payment of salaries, superannuation, leave calculations), financial matters (budgets, monitoring of expenditure) and records systems.

Examples of systems that rely on date-based calculations within the NSW public sector may include:

- booking systems (State Rail)
- offender management systems, staff rosters (Corrective Services)
- electricity payment systems (Energy Providers)
- student record systems (School Education)
- hospital waiting lists, immunisation reminders, staff rosters (Health)
- land tax, payroll tax revenue collection (State Revenue)
- licences (Roads and Traffic Authority).[12]

Consequence of Date-based Access /Control Systems

Time based access/control systems may affect:

- building services - electronics, building automation, security, fire, lift control and communications
- public utilities - water, electricity, lighting
- vehicle, shipping and aircraft control systems
- life support equipment.

The likelihood of systems failing depends on the degree of exposure and the preparedness of agencies (and Government as a whole) to address any likely problems.

---

[11] The DPWS has recently developed a methodology to assist agencies with these assessment processes. This is discussed in Chapter 4.

[12] It is important to note that the Year 2000 issue has been dealt with in regard to licences as these are already being issued for years beyond 2000.

1.4   Exposure Factors

Factors which affect exposure include:

- the nature of the business

- organisational characteristics such as a decentralised or centralised structure

- the nature, size and complexity of the IT environments used

- the nature of date-based control/access non IT and telecommunication systems used (affecting building services and medical equipment)

- whether resources (staff, finance and equipment) are available to resolve any problems.

This report examines the nature of the exposure and the likelihood associated with the Year 2000 problem. It assesses the effectiveness of what is being done compared to what can be done to address the issue at agency and whole of Government level.

Chapter 2 outlines the Year 2000 risks posed by the nature, size and complexity of the IT environments in the NSW public sector. It then examines the degree to which the agencies indicate they are prepared to deal with the Year 2000 problem.

Chapter 3 provides examples of risks posed by date-based control/access products and systems driven by programmable logic controllers (PLCs).

Chapter 4 examines major risks at the agency level and how they can be effectively managed.

Chapter 5 identifies the effectiveness of strategies that can be pursued at a whole of Government level to assist agencies reduce risk and resolution costs and, in so doing, reduce risks and costs to the State.

2. Risk to NSW: Information Technology

2.1   Introduction

This chapter outlines the IT environment in the NSW public sector and assesses where exposure to the Year 2000 problem is likely to be. The effectiveness of agencies' dealings with the problem and the effectiveness of strategies available to resolve any problems are then examined.

2.2   What Information Technology Could Be Affected?

The public sector IT environment is at risk in two major ways. First, particular forms of hardware and software pose particular problems. Second, the linkages in an IT environment will also determine whether an IT system will function correctly.

The NSW public sector has four major information technology environments. They are:

- mainframe

- VAX/VMS

- UNIX

- PC/Macintosh.

Mainframe, VAX and VMS are legacies of a previous information technology era where software languages such as COBOL and Fortran are not expected to be Year 2000 compliant. VAX/VMS environments have similar problems to those posed by mainframes. Critical business processes built on them have to be maintained. Therefore repair or replacement strategies will be needed.

UNIX is a disc operating system. The software and machines it runs on may need to be amended.

The life cycle of PC/MAC equipment means that replacement is more likely and therefore will be Year 2000 compliant.

One of the greatest challenges in a PC environment is the need to ensure that the hardware, software, application software and customisation are compliant together. It is only then that the system can be regarded as "compliant".

2.3 What IT Risks Does the NSW Public Sector Face?

Exposure

Four features of the public sector IT environment are important in terms of Year 2000 issues. These are:

- mainframes
- mid-range computers
- microcomputers
- application software.

The NSW public sector has a small number of mainframe computers (35 spread across 16 agencies). They pose a risk because they are likely to use outdated languages and are likely to be located in agencies with high exposure to the Year 2000 problem.

There are 1007 midrange computer units distributed across 78 agencies. Midrange computers pose a risk because of in-house developed or modified systems and links to external systems.

Almost 80 per cent of agencies use a programming language in the maintenance of their existing software applications. The main languages used are Basic, Cobol and/or Powerhouse.

Seventy per cent of agencies use programming languages for new systems development. The main languages used are Powerhouse, Basic, C and Cobol.

In development of new software applications, outdated languages such as Cobol and Basic are still being used, perhaps because agencies are using old machines.

Many end-user developed applications written in the Cobol and Basic languages have not accommodated the Year 2000. Manual testing is required. However, staff who know the languages are in short supply because the languages are outdated.

The application of newer languages do not pose as many problems provided that they have been programmed in a compliant manner and they are not exchanging data with non-compliant systems. This needs to be tested in each instance.

There were approximately 90,000 microcomputers in use at 104 sites or agencies in the NSW public sector in 1996.

Almost 60 per cent of microprocessors are Intel 486 which must be upgraded or replaced while a further 23 per cent are Intel 386 which must be replaced.

Likelihood   In attempting to determine the likelihood of Year 2000 problems occurring, DPWS followed a generally accepted methodology. That methodology involved asking agencies to:

- complete an accurate inventory of all relevant IT resources
- undertake a robust process to assess the business risks of the relevant IT resources
- formulate a realistic problem resolution strategy arising from the risk assessment exercise.

DPWS issued a guideline in September 1996 on "Planning for the Year 2000" to all agencies specifying the following steps:

- *Inventory* - establish an inventory of all agency business systems, operating software and technology environments
- *Assessment* - assess each component of the inventory for Y2K capability
- *Planning* - develop a strategic and tactical plan to correct Y2K problems
- *Report to Government* - provide the GIMB with advice as to extent of agency and whole of Government impact of Y2K
- *Implementation* - implement the chosen solutions to address the Y2K problem.

All agencies were required to report by 29 November 1996 at the conclusion of the *Planning* step. Agencies were also informed that:

Once received, all returns will be consolidated to provide Government with:

- information on the extent of the problem for NSW Government agencies;
- potential strategies for addressing the problem; including
- any funding implications arising from the need for corrective action.

Consolidated information and proposed strategies will then be provided to all agencies.[13]

---

[13] Director-General of DPWS, letter to CEOs, 16 September 1996.

The objective of issuing the guideline was to provide all agencies with a structured approach to the problem and to develop an understanding of the Government's exposure to the problem.

There has been no official consolidated information released to date. The DPWS consider the quality of agency responses was variable and this poses problems in terms of validity and reliability of the data. This may be a reflection on the preparedness of the agencies and/or the form in which reporting was required.

It is therefore difficult at this stage to evaluate the extent or likelihood of Year 2000 problems occurring. Agency responses to the DPWS' request for Y2K information indicated that, from 56 agencies:

- 5 agencies had high exposure, 15 had medium exposure and 32 had low exposure, with 4 having unkown exposure[14]

- total estimated cost $66m, half of which is for the Health related agencies

- approximately half of the agencies which reported a medium or a high exposure were still assessing their likely costs of compliance

- around 70 per cent of the agencies were still to estimate their costs of compliance.

In view of the above, little meaningful whole of Government information (eg total costs) can be inferred or extrapolated from the responses. A more rigorous approach in identifying the problem is needed to produce meaningful whole of Government information on the Y2K problem.

In-Depth Case Studies

To explore the issues further, two in-depth case studies were commissioned by The Audit Office and DPWS. These case studies identified a similar approach to Y2K in that both agencies:

- were aware of the Y2K problem and have allocated resources to tackle the problem

- have prepared inventories of "relevant" IT resources

- have attempted to assess the Y2K impact and develop problem resolution strategies

- have attempted to estimate the likely costs of compliance.

---

[14] DPWS unpublished analysis

However for both agencies, additional:

- resources are likely to be required to project manage Year 2000 strategies. A more structured and whole of agency approach to the problem (ie. not restricting the problem to merely the IT function) is required than has been the case previously

- research is needed on the inventories to ensure completeness and accuracy (eg there is a need to include all business equipment that have embedded date dependent microprocessors)

- work is required on the assessment process so that the Y2K problem and solutions are considered in the light of the agencies' and the Government's business risks

- investigation is required to estimate the final total costs of Y2K compliance (eg need to include time and cost estimates for problem identification, resolution and testing).

It is not unreasonable to infer that many other agencies are:

- at a similar stage of preparedness

- grappling with similar challenges in dealing with the Y2K problem.

However, the audit cannot identify from these two case studies or other information any reliable whole of Government estimates of the Y2K exposures and costs.

2.4 Strategies to Reduce Risk

Based on the above IT profile, the following general observations on Y2K can be made:

- in-house developed older (legacy) systems which are more prone to the Y2K problem are limited in number in the NSW public sector. Therefore, replacement strategies may not be as extensive as first expected

- there is a trend to use package software. This suggests that an *upgrade or replacement* strategy is more likely than a repair strategy for Y2K compliance

- the high number of personal computers suggests that there may be a high degree of *end-user computing*. Agencies may find it difficult to assess Year 2000 problems because end-users may have modified applications in such a way as to render them subject to Y2K problems.

Compared with a repair strategy, an upgrade/replace strategy is:

- less dependent on IT personnel resources
- subject to greater vendor control in terms of a product roll-out timetable
- more dependent on the vendor to test and prove Y2K compliance
- more reliant on central IT acquisition policies and practices (eg Government Standard Application Systems (GSAS) products).

If central IT acquisition policies and practices are to play a pivotal role in addressing the Y2K problem, consideration needs to be given to the appropriate roles and responsibilities of Government in regard to:

- future central IT purchasing decisions regarding Y2K compliance
- existing IT term contracts - assistance and advice to agencies on problem resolution
- Government "liability" regarding previous IT acquisition policies and practices
- funding considerations for agencies.

Emerging Issues   There are two emerging issues that warrant mention, IT outsourcing and mutual compliance.

IT Outsourcing   There has been a growing trend in the NSW public sector to outsource (parts or whole of) IT operations of an agency. It should be noted the outsourcing of IT operations does not absolve an agency's responsibility to address the Y2K problem and associated risks.

While outsourcing may allow an agency to access IT resources and expertise that it otherwise does not have, it does not automatically reduce or eliminate the Y2K problem.

Therefore, agencies should be cognisant of the Y2K problem in any outsourcing negotiations and adequately address the issue in any service or performance level agreements.

Mutual Compliance   As agencies are increasingly connected to each other through electronic commerce or simply exchanging data via physical media, it is essential that agencies are satisfied on the matter of "mutual compliance". That is, one agency's business functions should not be adversely affected by another agency's inability to provide Y2K compliant data.

The above issues are addressed in Chapter 5 of the Report as part of the whole of Government strategies to the Y2K problem.

3. Risk To NSW: Building Services And Medical Equipment

3.1   Introduction

This chapter examines two examples of important areas where Y2K exposure is possible: building services and medical equipment. Each area is examined in terms of:

- how it could be affected by Y2K

- possible exposure to and consequences for the NSW public sector

- preparedness of agencies to deal with this exposure

- strategies to address these issues.

Building services and medical equipment have been identified by DPWS as being vulnerable to Y2K problems.   They are examined here to highlight the need for a rational approach to the identification, assessment and resolution of Year 2000 problems. It is emphasised that this analysis is not meant to be a comprehensive audit of building services and medical equipment, but rather to illustrate Year 2000 issues.

3.2   Building Services

3.2.1   What Building Services Could be Affected?

Building services include:

- electronics

- building automation

- security

- fire

- lift controls

- communications.

At the commencement of this audit, DPWS was not in a position to provide to The Audit Office generic information about the Year 2000 status of various types of building services and commonly used products. State Property has now formed teams to address the Year 2000 issue and is currently working on Year 2000 implementation strategies to inform agencies about building services issues and products. These strategies will reduce duplication of agency effort in identifying and rectifying Y2K problems.

The Audit Office therefore wrote to a number of peak bodies and major industry suppliers to determine whether key forms of building services would be affected by the Year 2000 problem. The responses indicated that Year 2000 problems were neither universal nor "disastrous". Rather, any problems were quite specific, would not automatically affect the operation of products and services and, with good analysis of the problem and with good management, any major difficulties could be overcome.

For example, building services systems, although usually designed to last only 10 years, are likely to have specific problems in the areas of:

- fire systems which are not up-to-date in terms of IT (eg alarms are not transmitted across fibre)

- interfaces which will affect an application not the data itself

- contracts where companies may no longer be in business.[15]

Details of how fire alarm services, lift operations and communications for example, may be affected are outlined in Attachment 3.

3.2.2 What Building Services Risks does the NSW Public Sector Face?

Exposure

A complete database on suppliers of building services in the NSW public sector is not kept centrally. Various ownership and management arrangements of Government property would seem to be a contributing factor.[16] Government office accommodation serves as an example. Approximately 50 per cent of Government office accommodation is owned and managed by Government, the other 50 per cent is leased. DPWS on behalf of Treasury manage one third of this property (Crown Property Portfolio). Knight Frank Ltd. undertake the day-to-day management of this portfolio on behalf of DPWS.

It is impossible therefore to determine, as it is with IT, the nature of the building services environment and whether that environment has particular kinds of services or products that expose the State to risk.

---

[15] Audit Office interview with the company that manages property on behalf of the largest property owner in Australia.

[16] Although consolidated information was sought on building services in the Government property, specific advice from DPWS regarding the CPP (managed by Knight Frank) was received on selected properties and services.

Likelihood   The results of the DPWS' analysis of the Y2K status of agencies referred to in Chapter 2 indicate agencies have provided little or no information on their building services.   Therefore, it is difficult at this stage to determine the State's preparedness to deal with any Year 2000 issues in regard to building services.

3.2.3   Strategies to Address Building Service Issues

There is a need to manage Year 2000 building service issues differently, according to whether buildings are:

- owned and managed by Government

- owned by Government but managed by subcontractors

- leased.

Regional (country) NSW accounts for 79 per cent of owned office accommodation (number of properties) and just under half of the accommodation that is leased.[17]   The issue of whether regional NSW has access to the information and expertise needed to resolve any Year 2000 problems needs to be considered.   This may influence decisions about the nature and priorities of Year 2000 strategies.

In the first scenario, where the State is direct owner and landlord an audit needs to be conducted of buildings to determine whether they have systems that expose the State to risk.

The Crown Property portfolio (comprising around 30% of total Government accommodation of 1.14 million square metres) comprises six portfolios.

Treasury has notional landlord responsibility for all multi-tenanted government-*owned* properties and head lessor status in respect of all multi-tenanted *leased* premises.

---

[17] Source: DPWS GOA Database.

[18] The buildings in the Crown Portfolio (CPP Portfolio) include:

- Bligh House, 4-6 Bligh Street
- Chief Secretary's Building
- Education Building, 35 Bridge Street
- Goodsell Building, 8-12 Chifley Square
- Museum of Contemporary Art, 140 George Street
- State Bank Centre, 52 Martin Place
- St. James Centre, 107-111 Elizabeth Street

State Property (part of DPWS) manages the Crown Property Portfolio (CPP) on behalf of Treasury under a five year management agreement entered into in late 1993. Knight Frank Pty Ltd manages owned property and property leased on behalf of other agencies, for State Property. State Property directly manages heritage property and industrial land holdings.

In the second scenario, where the State has contracted the landlord function to a managing agent, there needs to be in the contract with the agent a clear responsibility for identifying and resolving any Year 2000 problems.

In the third scenario, where the State leases property, leases need to contain arrangements for taking responsibility for and resolving Year 2000 problems.

In terms of leasing, clearly there is an immediate opportunity to address any Year 2000 problems when renewing lease agreements because:

- 24 per cent have expired although premises are still occupied by Government agencies on a day-to-day basis

- almost 20 per cent of leases expire this year (a peak year in terms of the Government's lease profile).

Renegotiations of those leases which are due to expire between 1998 and the end of 2000 (68%) will also need to consider Year 2000 issues.

The above issues need to be addressed in improving the effectiveness and efficiency of management with respect to building services.

3.2.4   Recommendations

It is recommended that:

- up-to-date information about key building services areas where there is a risk be collected centrally and disseminated to agencies

- Year 2000 building services issues be managed according to the ownership/leasing status of properties and consequent responsibility arrangements

- there be consistent reporting on these areas of building services as part of the set of services and products controlled by at risk PLCs

- a standardised agency reporting format be developed allowing for the identification of the risk faced by services and equipment (including building services) (see Chapter 5)

- there be centralised and standardised monitoring and reporting of agency progress on resolution of all areas affected by Year 2000 problems including PLCs (see Chapter 5).

3.3   Medical Equipment

3.3.1   What Medical Equipment Could be Affected?

NSW Health has identified two broad categories of risk relating to medical equipment. The first is date-dependant biomedical equipment which is typically small, stand-alone equipment used for a variety of purposes in most hospital departments. The second includes other medical equipment such as medical imaging, nuclear medicine, radiotherapy, and laboratory equipment. The latter group tend to have complex computerised control systems.

In reviewing automated medical equipment, a NSW Health consultancy report (the Health report) prepared in November 1996 identified Year 2000 problems and their prevalence as set out in Table 3.1 below. It indicated that Year 2000 problems may be focused on particular classes of medical equipment.

The NSW Health report indicated that a strict compliance program should be required for all biomedical equipment and online patient management systems should have "special vigilance and testing". Among the systems requiring this vigilance were:

- medical imaging systems

- laboratory instrumentation (especially where packaged with PC controllers)

- radiotherapy systems

- critical care patient management systems

3.3.2 What Medical Equipment Risks does the NSW Public Sector Face?

Exposure

Like building services, there is no central inventory of equipment used in the public sector. Individual agencies are charged with the responsibility of managing their own inventory of assets. Large and decentralised agencies such as NSW Health cannot maintain equipment inventories centrally.

The NSW Health report was commissioned for this reason. The areas of possible exposure have been outlined above. There are other factors which increase this exposure apart from the Year 2000 compliance status of the equipment itself. These factors are:

- the effort (time and personnel cost) required to:
    - raise awareness of Year 2000 compliance
    - complete and maintain inventories of equipment and systems at possible risk
    - complete the assessment process and develop plans in conjunction with suppliers
    - achieve supplier co-operation, to work with central agencies and to disseminate information on Year 2000 compliance
    - ensure equipment is upgraded
- record, monitor and report on progress in implementation.

- the cost of replacement or upgrading of equipment which cannot handle the change to Year 2000

- areas which have potential to cause unexpected cost including:

  - expensive equipment that will be in service into or beyond Year 2000 and where the control system is customised to a particular site, is obsolete or not regularly updated as part of a maintenance contract[19]

  - data communications equipment and network management systems.

Likelihood

Likelihood of Year 2000 problems should be reduced given:

- co-operative arrangements between Government agencies and professional bodies

- a structure and process that maximises information sharing and reduces duplication of effort.

The Health report indicated medical equipment is already the subject of intense regulation, designed to be fail-safe and is regularly replaced. Because it is regularly maintained and inspected, many Year 2000 problems may be resolved through maintenance arrangements.

NSW Health and DPWS believe, however, that reliance on regulation and maintenance may not be sufficient to prevent occurrence of Year 2000 problems. As a consequence, NSW Health has designed a Year 2000 Date Issue Project to address statewide Year 2000 issues indicating that they are exercising due diligence to avoid foreseeable problems. The project has the following objectives, namely to:

- co-ordinate the identification, development, and communication of appropriate Year 2000 strategies, guidelines, checklists, vendor status, action plans and standards

- provide advice, assistance, co-ordination and support for Statewide and Area Year 2000 Committees to increase awareness, ensure responsibilities are known and commitment maintained

- co-ordinate and manage Area activities in terms of identifying and resolving Year 2000 problems.

---

[19] This includes medical imaging systems, laboratory instrumentation and building/security control systems

The NSW Health Year 2000 Project is supported by a Steering Committee with broad representation from the Department, Areas, IT, bio-medical engineering and building maintenance.

Biomedical Equipment

The College of Biomedical Engineering (Institution of Engineers) under the leadership of biomedical engineers from NSW Health is developing test protocols and testing biomedical equipment.

The College is establishing a national database of medical equipment that has been tested for immunity to the Year 2000 bug. The purpose of the "clearing house" database is to provide a central source of information that will enable persons involved in assessing equipment to identify quickly whether a particular type and model of equipment has already been assessed.

NSW Health has created an Internet page with the assistance of DPWS. This includes testing criteria, and extracts from the database in various sequences. Information for the database is being collected from biomedical engineers throughout Australia and elsewhere and forwarded to a regional health service where the information is being validated. The database is then updated with this information.

Local databases will also be created for each hospital, with a record for each piece of equipment.

Other Medical Equipment

NSW Health has engaged specialist consultants to survey other medical equipment to identify potential problems and to recommend appropriate testing and remedial work. The reason for this approach is that "biomedical engineers typically do not handle the equipment used in medical imaging, nuclear medicine, radiotherapy and laboratories."[20] The testing will initially be carried out in two pilot projects. This will form the basis on which an approach for compliance assessment throughout NSW Health will be developed. There will also be a central "clearing house" database for this medical equipment.

Close co-operation with equipment suppliers and their agents is expected in this assessment and remediation exercise. Where this is not possible, consultants and hospital engineers will carry out remedial work.

---

[20] NSW Health letter to NSW Audit Office 3 October, 1997.

Legacy Systems   All legacy application systems are being rectified to be Year 2000 compliant. A central testing facility is to be established to enable comprehensive testing of all legacy and statewide systems.

Area Health Services   Area Health Services are responsible for carrying out their own Year 2000 projects which include risk analysis of business systems and locally developed application systems. The DPWS methodology for risk assessment and Year 2000 project management is being used.

Areas are supported by the NSW Health statewide project to assist co-ordination and avoid duplication of effort between hospitals.

Review   Reviews or audits will be carried out to ensure the completeness and thoroughness of plans and remedial actions. Area projects will be reviewed by the statewide project team for adequacy and timeliness, with exceptions and issues being reported to the Statewide Year 2000 Steering Committee.

The statewide strategies and project plans will be subject to review by an external consultant to ensure that the scope is adequate and that the approach is appropriate. It is also intended to establish a "partnership" with a legal firm, which would provide advice and briefings and which would monitor plans and activities to assess any potential legal implications. The statewide project will also be subject to review by DPWS as part of its strategy of checking agency Y2K compliance processes.

3.3.3   Strategies to Reduce Risk

NSW Health is already implementing most of the recommendations of the NSW Health report. Additional strategies have been implemented beyond these recommendations to ensure all possible steps are taken to identify and resolve Year 2000 problems.

Summary   In summary, some forms of building services and medical equipment are believed to be at risk of Year 2000 problems. These and other non IT systems and products which are affected by PLCs will need to be checked and tested for their Y2K vulnerability. Peak industry or professional bodies can clearly assist with this exercise.

Table 3.1 : Examples of Medical Equipment and their Year 2000 Exposure[21]				
System	**Example**	**Prevalence**	**Problem**	**Resolution**
Complex Systems	PABX and associated equipment	22%	Expensive real-time systems; critically dependent on date/time functions	Covered by regular maintenance contracts; most manufacturers aware, assessing problem and developing resolution plans
Electromechanical equipment	Simple data logging systems; monitoring devices; eg security control systems[22]	11%	Almost all dependent on date/time function; Most PCs as a computer platform only partially compliant	Equipment controlled by dedicated PCs Usually covered by maintenance agreements covering faults and hardware failures, do not cover regular software upgrades; co-operative arrangements could help limit exposure.
Electromechanical equipment with in-built microcontrollers	Components in larger systems eg communications controllers; entire systems eg laboratory instruments	30-40%	High levels of date/time compliance as in data communications equipment (largest group in this class)	Not stated
Simple devices with in-built date/time functions	Expiry date ticket printer only item in this class to have critical date printer	Not stated	Devices hold date and time for recording or display purpose	Not stated

---

[21] DH4 Pty Ltd.
[22] Included in building services earlier in this chapter

4. Agency Strategies to Reduce Risks and Costs

4.1 Introduction

This chapter summarises the problems agencies face in terms of the risk factors and their resolution for the Year 2000. The chapter then outlines how agencies might address these problems to reduce risks and costs. The chapter draws on both the literature and case studies of two NSW Government agencies that were subject to review by external consultants. The aim of these case studies was to determine the relative risk and potential cost implications agencies faced in dealing with the Year 2000 problem.

4.2 The Case Studies

In co-operation with the DPWS, The Audit Office engaged consultants to review two NSW Government Agencies.

Two aims of the case studies were to:

- review the activities performed to date by the agency to enable a high level assessment to be made of:

    - the extent of the Year 2000 problem

    - the likely cost of correcting the problem

    - the current state of preparedness

- identify a number of effective, whole of Government strategies necessary to address the Year 2000 problem.

Case Study A (by Coopers and Lybrand) reviewed an agency with one large central office and four regional sites. It is heavily reliant on mainframe technology for its operations.

Case Study B (by EDS Consultants) reviewed a smaller decentralised service delivery agency. It has a head office in Sydney and a statewide field establishment of four Zones and 27 Districts, grouped into six Regions. The many dispersed locations are networked via PC-based equipment and are reliant on such technology for data sharing and data communications throughout the agency.

4.3 Issues Facing Agencies in Resolving Year 2000 Problems

The literature and the case studies identify the following key problems facing agencies in dealing with the Year 2000 problem:

- lack of awareness of the Y2K issue

- lack of a business risk culture that would recognise Y2K as a business issue

- nature of the organisational structure

- the need for asset management that is appropriate for the nature of IT, business and equipment environments

- need for recognition of agency dependencies

- need for project management across the agency

- difficulties in defining resolution costs

- difficulties in managing business resources.

4.3.1 Lack of Awareness of Issue

A high level of awareness of the Year 2000 problem is needed throughout an agency assisting in the identification and resolution of any Year 2000 problems. The consultants' case studies indicated that there was considerable awareness at executive level, heightened by the conduct of the case studies themselves. Both case studies found there was less awareness at lower levels of the organisation.[23]

The case studies have also identified the need to increase awareness of end-users, especially if they:

- have developed systems containing vital business information

- use outdated and redundant versions of software.

The literature and case studies emphasise the need to address this problem through an awareness campaign *within* organisations. However, there is less guidance in the literature on the criteria for a successful campaign, its scope and target audience.

---

[23] EDS, "Year 2000 Diagnostic Review", 1997,p.1; Coopers and Lybrand, "Year 2000 Diagnostic Review", 1997, p.10.

The Coopers and Lybrand Report provides some examples of awareness and education campaigns that might be considered:

- publication of articles on the issue and progress to date in internal newsletters

- communication of project progress using electronic mail

- publication of a Year 2000 project newsletter

- discussion of the Year 2000 issue in management training and conference forums

- presentations at divisional meetings

- conduct of Year 2000 training sessions throughout the organisation

- "brainstorming" the business impact of Year 2000 in team and business meetings.

Case B, like many other agencies, distributed to all agency staff an Information Leaflet prepared by DPWS to raise awareness. This leaflet is being used with other measures to maintain awareness within the agency.

4.3.2   Lack of Recognition of Issue as a Business Issue

The business and industry literature emphasise the need to regard the Year 2000 problem as a business issue rather than being the responsibility of the IT section alone to manage.

From a business perspective, Case Study A identified the following impacts:

- customer service

- employee morale

- public image

- client confidence

- financial control

- financial reporting.

While every agency could have "unique" impacts by virtue of their business operations and services, Case Study A identified "generic" areas that could be affected:

- payments to beneficiaries and suppliers

- provision of acceptable levels of operational service to the public

- collection and monitoring of revenue

- response to enquires from the public and other bodies in a timely manner

- compliance with legislative requirements

- payment of staff

- preparation of financial and management reporting.

Various factors affect the nature and extent of the risk. These include:

- nature of the business, its size and complexity

- the *pervasiveness* of the problem which may affect all information systems, together with environmental and facilities' systems and equipment and user developed spreadsheets and models[24]

- the need to remain flexible and responsive to Government policy which may require modifications of systems.

In Case A the efficient and effective conduct of the business is totally dependent on the functioning of IT systems. Any IT failure or the inability to respond quickly to changes in Government policy will:

- disadvantage customers requiring legal documents to be processed by that agency

- have short and longer term impacts on the efficient collection of revenue for the State.

Key business processes in Case Study B could feasibly be conducted using alternate methods. Failure, at least in the short term, would therefore pose only a moderate to low level of risk to the agency, to customers and to the State.

---

[24] Coopers and Lybrand, 1997.

Essentially, business decisions need to be made about:

- what operations are important to the business

- what processes support these operations

- which of these might be affected by the Year 2000 bug

- what impact there would be if processes failed

- what alternative resolution strategies are available and what is their cost

- how these strategies might impact on other business decisions and other projects

- how resolution strategies fit with overall asset management plans

- the need for involvement of staff at all levels in risk and project management.

As a business issue, there is a need to recognise the management of the Year 2000 problem as *a risk management exercise*.

This has three implications in that agencies:

- should remove from the scope of resolution strategies business units and/or technology components that are not essential for ongoing operations[25]

- need to put in place effective systems of internal control and internal audit

- should publicly report their assessment of risks posed by Year 2000 and the controls and strategies they have in place to manage risk.[26]

4.3.3   Nature of Organisational Structure

The nature of organisational structures and the degree of standardisation of their IT systems significantly affects the ability to manage the Year 2000 problem.

Case B is a decentralised agency with offices and officers dispersed across the State. This can create difficulties in creating awareness, developing an inventory, undertaking assessments and therefore in identifying appropriate resolution strategies.

---

[25] The Australian National Audit Office is proposing that Commonwealth agencies treat Year 2000 as a risk management exercise and follow the standard process of: establishing the organisational context for the analysis; identifying risks; analysing risks; assessing and prioritising risks; treating risks; and monitoring and reviewing remedies.

[26] The issue of reporting is discussed in Chapter 5.

Clearly, the nature of organisational structure needs to be taken into account when formulating resolution strategies.

A strength of Case B was that the setting of, and adherence to, standards and purchasing IT goods and services centrally significantly reduced the extent of risk.

4.3.4   The Need for Asset Management

IT Environments

The Year 2000 assessment of infrastructure and facilities should be regarded as a trigger for the introduction of improved asset management practices:

- all new purchases (of IT and non IT equipment) should be Year 2000 compliant and should meet standards (see Chapter 5)
- any new system should be Year 2000 compliant
- centralised control of products used in multiple business units assists with achieving compliance
- registers should include information about compliance.

The case studies confirmed that different environments, especially IT, pose different resolution problems. Case A with mainframe legacy systems means that replacement/repair will be the major resolution strategy.

Case B with its PC based environment faces a greater end-user compliance problem. Seven problem domains and their associated risk level are shown in Table 4.1 below.

Table 4.1 : PC Domains and Their Level of Risk	
Domain	**Risk Level**
Centralised Applications	Moderate
End-user Applications	Moderate
Computer Platforms	Low
Computer Networks	Moderate
Externally provided Software	High
Infrastructure & Facilities	Moderate
Business Processes	Low

The consultant's report confirms The Audit Office's analysis that the problem in a PC environment is a lack of end-user awareness. The report recommends that this problem be addressed by system liaison units:

- raising awareness of the problems associated with spreadsheets

- assisting in the identification of business critical spreadsheets

- providing support to the users who would change the spreadsheets.[27]

Given the possible importance of business critical spreadsheets and user developed applications, the consultant's report recommends that these be placed under the control of an IT division. A more fundamental issue is that information critical to the business should be on a business system and be controlled by the business.

Version control and release procedures

Both case studies indicated that there could be a risk to operations caused by lack of version control. In Case B, of 168 commercial software packages in use, 128 are specialist packages which have fewer than five users.[28] These packages are required because of the diversity and specialised nature of the functions performed by the agency.

The consultant's report recommended this problem be overcome by agencies reviewing version control and release procedures to ensure they support co-ordination between applications.

4.3.5 Need for Recognition of Agency Dependencies

Business Partners

There is a need to recognise that the interaction of an agency with external suppliers and other agencies (in terms of IT and non IT products and services) will impact on risk.

---

[27] Coopers and Lybrand, 1997, p.38.
[28] Letter from Case B agency to The Audit Office, 3 June 1997.

In terms of software, hardware and service suppliers, there is a need to:

- investigate the degree of compliance of vendor supported systems and pieces of equipment[29] in a systematic and rigorous way. The following information would be required:

    - version number of proposed Year 2000 compliant release

    - expected date of Year 2000 compliant release

    - method used by the vendor to achieve compliance

    - date format used by the product

    - costs of upgrading

    - vendor testing and quality assurance performed to verify Year 2000 compliance.

- incorporate into upgrade planning and implementation and testing schedules vendor delivery of promised products, compliance and compliance testing

- consider the option of centralised investigation and negotiation with suppliers for commonly used products in order to reduce the cost of addressing this risk (see Chapter 5).

Interfaces   In terms of interfaces, there is a need to identify:

- in-house system interfaces for incoming data

- in-house system interfaces for outgoing data

- external file transfers for incoming data

- external file transfers for outgoing data.[30]

Case A receives data from eight government (Commonwealth and State) agencies. If these agencies do not address their Year 2000 problems in a manner that is timely, effective or consistent with Case A's approach, there will be an adverse impact on the agency's operations.[31]

recommends that Case A should ensure information:

- providers are taking action to address Year 2000 issues so they can continue to provide valid information

- will be provided with a century format that is acceptable to the agency's compliant systems.

---

[29] See for example Coopers and Lybrand, 1997, p.25.
[30] SOCITM "Year 2000 Working Party:Bulletin Number 2".
[31] Coopers and Lybrand, 1997, p.44.

4.3.6 The Need for Project Management

Both evaluations highlighted this need for the Year 2000 problem to be managed as a project.

It was recommended that there should be:

- high level sponsorship reflecting the Year 2000 as a business issue

- enterprise wide, not just IT responsibility for aspects of the project. Business unit managers should be required to report regularly on the Year 2000 status of systems and sign off as they become compliant

- strong project management because of:

  - the fixed deadline

  - a need to maintain close integration with other agency projects

  - a need to manage complex interfaces and application coordination that arise as individual systems are made year 2000 compliant

  - little or no scope for error in changes that are made

  - likely resource shortages

There was also a need to address:

  - Year 2000 compliance definitions

  - acceptance criteria

  - approaches to inventory and assessment

  - accountability

  - required standards and procedures

  - resourcing strategies

  - testing strategies.

4.3.7 Difficulties of Determining Resolution Costs

It is impossible at this stage to identify the level and nature of Year 2000 costs for the NSW public sector (see Chapter 2). This is because are many agencies have not yet:

- accurately identified Year 2000 problems

- recognised the need to include non IT problems in their assessments

- evaluated their dependence on other agencies or suppliers

- been able to identify what resolution strategies they need to adopt.

4.3.8   Difficulties in Managing Business Resources

The literature and the case study evaluations emphasise the risks to business imposed by the need to manage resources more efficiently and effectively in a time of fiscal constraint. The risks here include:

- shortage of time

- volume of transactions

- thoroughness of checking required

- shortage of personnel

- shortage of service specialists

- lack of availability of tools for problem identification and conversion

- considerable cost of resolution

- increased workload on users

- funding shortages.[32]

4.4   Recommendations

To reduce risks and costs within relevant agencies, it is recommended that they:

- develop an internal awareness campaign for all staff

- recognise Y2K as a business issue

- treat Y2K as a risk management exercise

- utilise a project management approach such as the one developed by DPWS to identify, assess and address risks.

---

[32] "Future Shock cushioned packed" The Australian 22 April 1997, p.10 and Coopers and Lybrand,1997, p.37.

5. Whole of Government Action to Reduce Risks and Costs

5.1 Introduction

This chapter identifies areas which the NSW Government could address to reduce risks and costs to agencies and the State. It evaluates State Government action to date and suggests future strategies.

To improve effectiveness, there is a need for a more comprehensive approach to Year 2000 issues which includes:

- a more precise identification of State wide risks

- a more strategic approach and appropriate structure

- development of a consistent definition of Year 2000 compliance and criteria for use, where appropriate

- management of purchases (tenders) and contracts

- financial matters

- legal considerations.

5.2 Government Approach (Roles and Responsibilities)

Resolution strategies need to be developed within a policy approach that defines:

- the roles and responsibilities of Government, its central and line agencies (including an appropriate supportive central structure)[33]

- the scope of the policy

- the definitions and criteria/conditions of Year 2000 compliance to be adopted

- the roles and responsibilities of agencies impacting on Year 2000 strategies

- contract management and purchasing matters

- funding principles and treatment of resolution strategies

- approach to agency line support

- preferred approach to resolution strategies

- Government position on legal matters such as intellectual property, liability and supplier responsibilities.

---

[33] The Australian National Audit Office are examining this issue in terms of corporate governance principles of: leadership, statutory accountability, communication with stakeholders; roles and responsibilities; accountability for resources; internal controls; committees; and reporting.

Approaches to resolving the Year 2000 problem adopted by other jurisdictions lie along a continuum of assistance or intervention. Approaches include:

- no/little intervention or assistance

- facilitating agencies to resolve problems by providing centralised support and individual guidance

- compliance through semi-formal arrangements such as CEO Performance Agreements and monitoring

- interventionist approaches which include a legal dimension such as introducing legislation.

Approach 1: Agency Responsibility

Victoria   Of all jurisdictions within Australia, Victoria has adopted the most "laissez faire" approach. Its position is that each agency "is responsible for its own service delivery and therefore all issues connected with Year 2000-data processing are the responsibility of respective CEOs".[34] It is expected that CEOs might incorporate it in their business plan which is discussed every six months with the Premier.[35] Some assistance has been offered by the Department of State Development which has provided guidelines on warranty clauses.

Approach 2: Central Role in Facilitating Resolution

British Columbia   British Columbia has adopted a centralised, multi-faceted approach to *assist* agencies resolve the Year 2000 problem. It combines central support and monitoring as well as individual agency support. The approach is one of the most proactive, strategic and comprehensive of all jurisdictions examined in this audit.

---

[34] Victoria Year 2000 Tasks Home Page; Audit Office communication with John Best, Multimedia Victoria 30 July 1997.
[35] Beyond this, there is an informal structure for sharing of Y2K experiences (Year 2000 special interest group) and some assessment of three agencies. Several agencies are currently undertaking their own assessments.

British Columbia's Information Technology Access Office (ITAO) formed a Year 2000 Task Force. Its role was to advise Government on an appropriate framework "to ensure that any Year 2000 issues do not disrupt service to the public and cause any more expense to government than warranted".[36] *It was believed that a framework was required to ensure government agencies were not "'re-inventing the wheel' in evaluating tools and methodologies to address the Year 2000 systems issues".* (emphasis added)[37]

The Task Force recommended a whole of Government approach to the Year 2000 issue. This would co-ordinate effort to provide maximum support and guidance across central agencies as well as economies of scale in resolving problems.

Specifically, the Task Force recommended:

- the development of a policy document that clearly defined the roles and responsibilities and liabilities of key central agencies

- the establishment of a Year 2000 Implementation Task Force responsible for:

  - proposing a uniform date standard (possibly ISO 8601)

  - identifying cross-government common infrastructure or tool requirements

  - monitoring and reporting on overall Government progress every six months

  - facilitating agency activity

  - co-ordinating agency activity in terms of sharing or evaluating tools, undertaking pilots and sharing costs

  - reviewing "test environment options" and co-ordinating timeframes and schedules

  - developing a website bulletin board to communicate to agencies and share information or issues

  - managing vendor information which should be updated six-monthly.

Each agency had the responsibility of developing a three year Y2K plan (updated annually) and identifying a Year 2000 project manager. The project managers were to be members of the Task Force and were charged with the responsibility of ensuring agency compliance.

---

[36] Information and Technology Access Office (ITAO) "Year 2000 Task Force Review of Year 2000 Systems Issues in the Government of British Columbia" July 26 1996.
[37] ITAO, loc. cit.

Tasmania and South Australia   Within Australia, the Commonwealth Government and the Tasmanian and South Australian Governments have adopted a facilitation approach. In many respects, the approach of these jurisdictions is similar to that adopted by British Columbia. It is also broader and more strategic than that adopted by NSW (see below). (Attachment 4 provides a summary of Commonwealth and States' actions.)

The Commonwealth Government has a complex structural arrangement because the Government has sought to:

- establish a mechanism to support its own agencies (in terms of creating awareness, surveying Y2K readiness, and developing reporting procedures)

- work with the States to provide regular briefings to a Commonwealth/State Committee of Ministers for Communication (Online Government Council).

Features of the structural arrangements for the Commonwealth are:

- the Office of Government Information Technology (OGIT) has a Y2K Committee which reports through a Policy Advisory Committee to the Minister for Finance, Minister for Science, Industry and Tourism and Minister for Consumer Affairs

- this Y2K committee, to date, has included the Australian National Audit Office

- a quarterly forum for Commonwealth agency representatives to share ideas on Y2K issues.

The Commonwealth's strategies have been supported by a very precise definition of Year 2000 compliance and by standards (see 5.4 and Attachment 4).

As is the case in NSW with the DPWS' GIMB, the Commonwealth IT & T Policy Advisory Committee involves industry.

The Tasmanian Government's key initiatives include central structural support, information, legal and industry strategies. Similarly, South Australia has taken a strategic, facilitation approach. Year 2000 standards have been formulated and structural, scoping, information and industry strategies have been developed. The South Australian strategy is supported by a central agencies program.

This is a reference group which addresses whole of Government issues. The group comprises:

- Department of Information Industries

- Department of Treasury and Finance

- Crown Solicitor's Office

- Auditor-General's Department

- Department of Premier and Cabinet.

Like Queensland, there is a focus on financial and legal issues.

Approach 3: Semi-Formal /Semi-Interventionist

Western Australia

Western Australia has adopted a position where the Government will facilitate awareness and agency compliance, not legislate or require it. However, this "semi-formal" approach is more structured than those in Tasmania and South Australia. The approach places responsibility for resolution of Y2K problems on CEOs through its incorporation in their Performance Agreements. Ministers must be kept informed of CEO progress in identifying and managing risks.

The business risk management approach allocates clear responsibilities:

- CEOs are responsible for adopting appropriate policies, guidelines and practices

- managers are responsible for all processes and systems (in-house or contracted out), for all purchases of equipment and software and for staff awareness

- staff are responsible for their individual applications.

Effective and efficient Government support and monitoring are achieved by:

- determining priority areas such as purchasing, health and Worksafe

- requiring regular mandatory reporting to Government (via Premier's Department) on IT, areas that have embedded chips and business relationships

- reporting against agency specific risk management plans in annual reports, commencing 1996/97

- facilitating awareness through focus groups especially in high risk areas

- providing structural support, co-ordinated through the Public Sector Management Office and the Information Policy Council's Year 2000 Focus Group

- making the Minister for Commerce and Trade and Small Business responsible for communicating with the private sector.[38]

Queensland also has a centrally driven, structured approach to ensure there is a "consistent cross-government approach to each of the major issues".[39] A project office has been established in Premier's Department to addresses high level policy and guidelines.   As indicated above, the guidelines and checklists include information to agencies on:

- legal considerations

- directors' and Minister's duties

- procurement

- samples of letters to vendors

- intellectual property

- copyright matters

- litigation

- draft Year 2000 clauses for contracts.[40]

Approach 4: Interventionist/Legal Approaches

A legal approach to resolving the Year 2000 problem has been considered in New Zealand, the United Kingdom (UK) and Singapore and has been implemented, in interim ruling form, in USA.

New Zealand   In New Zealand a private member's Bill released for comment in April 1997 would require all Government departments, Ministries, State Owned Enterprises and companies among others to:

- undertake a Year 2000 audit of their computer systems including machines embedded with a semiconductor chip

- report on these audits

- report on proposed actions.

---

[38] WA Public Sector Management Office and WA Audit Office communications to NSW Audit Office. This includes Information Policy Council Policy Statement and Audit Office Background Paper, risk matrix and standard questions list issued to auditors.
[39] Queensland Internet Home Page 25 June 97.
[40] Audit Office phone conversation with Queensland Year 2000 Project Officer, 21 August 1997.

Reports would be provided to the Chief Executive of the Ministry of Commerce each financial year ending before 31 December 1999. The penalty for failure to comply would be $250,000 (US $175,000).[41]

USA

In the US there have been high profile Senate inquiries into this issue for some years.[42] The Senate has passed an interim ruling regarding the Year 2000 problem on 1 January 1997 as part of its efforts to define what Year 2000 compliance means.[43] A final ruling is expected during 1997.

Legislation has been complemented by a focus on policy development and co-ordination strategies, including:

- co-ordinating interagency operations by the Office of Regulatory Affairs (part of the Office of Management and Budget)

- specifying in contracts a definition of Year 2000 compliance

- requiring Year 2000 compliance when purchasing of new technology or of upgrades

- establishing an interagency working group on Year 2000.[44]

Other

Other countries including Singapore and UK have also been proactive with regard to Y2K. The Singapore Government is planning to introduce legislation forcing companies to become Year 2000 compliant.[45] In Britain a Companies (Millennium Computer Compliance) Act 1997 was drafted to require companies to conduct and report on an assessment of the Y2K capability of their computer systems. It also required reporting on actions directors proposed to take to resolve problems. The legislation lapsed with the calling of the General Election in February 1997.[46] The Government has also established a taskforce directed by the Heads of the Confederation of British Industry (CBI) which provides information and assistance to organisations on the Year 2000 issue.[47]

---

[41] Hon Peter Dunne "Millennium Computer Compliance Bill" United New Zealand.

[42] Margaret Banaghan "The looming computer disaster" BRW 19 May 1997 p. 49.

[43] David Binning "Y2K switch risk needs action:analyst" ComputerWorld 3 May, 1997, p. 12.

[44] Memorandum for Agency Chief Information Officers, and Senior Procurement Executives from Sally Katzen, Office of Information and Regulatory Affairs and Stephen Kelman, Office of Federal Procurement Policy, 9 January 1997; Statement of Sally Katzen to US House of Representatives, 10 September 1996.

[45] Margaret Banaghan "The looming computer disaster" BRW 19 May 1997 p. 49.

[46] Year 2000 Bill (internet site) Bill details.

[47] "Taskforce 2000" Website.

NSW Approach   NSW has developed a number of strategies based on an *implicit policy position which encourages rather than legislates for* Year 2000 compliance. The NSW position is a mix of support and "voluntary compliance". The strategy has four key elements:

1. an awareness campaign for public sector CEOs and agencies and private sector businesses

2. an information strategy

3. a risk assessment strategy for Government agencies

4. a resolution strategy using guidelines, contract management and "compliance" requirements.

Information   The issue of information has partly been addressed above. Agencies need information in regard to:

- products, services and equipment
- contract management
- legal/liability issues
- sources of support available
- technical issues (resolution strategies).

NSW strategies in regard to the first two issues have been outlined above.

Awareness   The awareness campaign to ensure all agency chief executives and IT managers were aware of the Year 2000 problem advising them of the intention to take a lead in addressing the problem[48] was launched in May 1996. Since that time it has comprised:

- the Director-General of DPWS writing to CEOs about Y2K problems

- liaison by the Director-General of DPWS with the Chief Executives Committee. This body advises the Director-General of Premier's Department

- raising the issue at the GIMB on which key line and central agencies are represented

- holding a Year 2000 summit

- developing a proposed State-wide educational program developed in conjunction with other State Government agencies for small business

- DPWS writing to all vendors who have products listed on the Government panel and period contracts requesting advice as to Year 2000 capability of their products and, if applicable, a planned timetable for the release of year 2000 capable versions. Information received was made available via the DPWS home page on the Internet.

---

[48] Alan Finegan "Speech to Year 2000 Summit", 24 June 1997.

Compliance There is considerable emphasis on compliance using a risk assessment and resolution strategy. The Government Information Management Division (GIMD) of DPWS has developed a four pronged approach to assist agencies (except for SOCs) to develop Year 2000 compliance strategies. This will include:

- assessment of the problem using contractors drawn from a panel

- rectification of the problem using approved contractors

- certification by DPWS that the process they have used to address the problem is acceptable to DPWS

- development of contingency plans.

To support this process, DPWS have developed a "Year 2000 Business Risk Analysis Handbook".[49] This comprehensive document will assist agencies in identifying risks, developing and implementing assessment, testing and resolution strategies. Effective use of this tool should:

- enable agencies to demonstrate that they have been diligent in addressing foreseeable risks (see section on legal issues)

- provide Year 2000 compliance information which is standardised across agencies and which can be used by DPWS to monitor and report on agency management and resolution of the problem.

Use of the "Year 2000 Business Risk Analysis Handbook" by agencies will also ensure that the information required to provide effective central support facilities is gathered, especially in terms of :

- agency risk exposure

- agency budgets

- details of impacted resources

- rectification requirements.

Structure In most other States, structural support for agencies from "whole of Government" has been located in Premier's Department. Some jurisdictions have, in addition or as an alternative, a central agency Working Party to provide leadership, direction and accountability for Year 2000 strategies.

---

[49] The Handbook is available on the Internet.

In NSW, responsibility for "whole of Government" initiatives and their implementation has been located in the GIMD in DPWS.   A unit within GIMD, with a budget of $ 0.5m per annum over three years has been established to ensure agencies:

- follow assessment and rectification procedures

- have these processes certified

- report centrally.[50]

The DPWS, in their lead role in addressing agency Y2K issues need active central agency support. First, DPWS needs support to continue its strategic approach to:

- identifying common needs

- designing whole of Government strategies according to risks posed by business functions or agency size

- investigating how resolution strategies and costs might be shared

- liaising with suppliers on a whole of Government basis.

Second, a central agencies program is needed to:

- investigate the issue of Y2K status of SOCs

- resolve significant sector wide financial issues associated with Year 2000

- develop an appropriate legal framework to address Year 2000 issues

- assist with co-ordinating a detailed industry and small business strategy.

---

[50] DPWS' strategies to assist agencies identify and assess their Year 2000 problems have included research redistributed to Government's website and the co-sponsoring of the two case studies used in this Report.

5.3   Identification and Reporting of Risks

In order to resolve the Year 2000 problem in the most effective and efficient way, it is essential that areas of high risk be identified. As noted earlier in this report, high risk areas include services which might affect health and safety and revenue raising activities.

As indicated earlier in this report, the DPWS had undertaken an evaluation of agency Year 2000 status and proposed resolution strategies. The survey requested information for each inventory (IT and non IT) item:

- assessment of Year 2000 capability

- scope of corrective action to be undertaken

- estimated cost

- likely timeframe.

The Department, as noted earlier in this Report, indicated to agencies that a consolidated report would be available and that a consolidated whole of Government analysis of results has been completed.[51]   However, the low number and poor quality of responses has prevented any meaningful analysis.

Most other jurisdictions have adopted a strategy of regularly monitoring and reporting on Year 2000 compliance across the public sector.

Reporting can take a number of forms, that is reporting:

- to Cabinet through DPWS (proposed NSW policy)

- to a central agency

- through an Annual Report, in terms of how risks are being managed

- in accord with Australian Stock Exchange (ASX) rules (Annual Report risk management strategies) where agencies are under *Corporations Law*[52]

- by way of a CEO Performance Agreement.

As indicated in Chapter 4, agencies should establish effective systems of internal control and internal audit to help manage the Year 2000 problem. In line with this, they should report on risk management activities in their Annual Report.

---

[51] DPWS speech to summit 24 June 1997.
[52] The latest Commonwealth Bank Annual Report specifically refers to Y2K risks.

5.4   Definition of Compliance

There is a need to have an adequate and consistent definition of Year 2000 compliance for the NSW public sector. This would be used in all tenders and contracts. Tenders would also require information regarding the conditions under which products and services would operate in order to achieve this compliance.

Other jurisdictions such as USA and industry and business are already using a clearly articulated definition of Y2K compliance.[53] Some jurisdictions have built it into purchasing contracts. EDS recommended that Year 2000 compliance definitions and clauses for contracts and purchasing agreements should be developed centrally and made available to all government agencies to incorporate into their own standards and procedures.[54]

The Commonwealth has been very thorough in considering technical and legal issues in their drafting of a Year 2000 compliance definition. This definition, developed by the Attorney General's Department, with input from OGIT, comprises definitions of products, valid dates, calculations, related products, compatibility and warrantee or guarantee. It is currently being reviewed with input from Purchasing Australia. [55]

Many suppliers have also been developing their own definitions. Some such as Telstra have supplemented this by specifying criteria by which all applications can be measured to evaluate if an application is fully compliant.

Currently in the NSW public sector, different definitions of Year 2000 compliance are being used or proposed. Examples include:

- State Contracts Control Board Contract (SCCB) makes it mandatory that any product offered in response to a tender is "capable of coping with the change of the century from the years 1999 to 2000 without modification or cost to the consumer"

- The Audit Office tender for Financial Audit Methodology

- Health.

---

[53] For example, communication from Telstra to Audit Office 21 July 1997.
[54] EDS recommendation, 1997, p.4.
[55] Phone Conversation with Commonwealth Attorney-General's Department which expressed concern that some definitions used in the IT industry or by peak bodies do not address the full range of Year 2000 compliance problems.

The DPWS established a committee involving State Supply and GIMD of DPWS as well as Crown Solicitor's to develop an appropriate definition of Year 2000 compliance. This definition will be used in all DPWS contracts including that used by the SCCB.

There is no clear rationale for different parts of the NSW public sector using different definitions of compliance. The legal implications of doing so need to be considered.

5.5   Legal Issues

Legal issues regarding the Year 2000 can be regarded from three perspectives:

- Government and the NSW public as customers

- insurers

- suppliers.

Government   DPWS believe that, from a Government and NSW customer perspective, risks of litigation include:[56]

- action against the Government for failing to deliver services due to foreseeable year 2000 failure

- Government being sued because a regulatory body fails to make organisations it regulates aware of or act upon potential problems caused by Y2K.

Agencies can address the first of these risks to Government by taking action to identify, assess and reduce risks through a Year 2000 certification process such as the one suggested by DPWS (see earlier section in this chapter). This methodology follows commonly accepted procedures in the IT industry.

According to DPWS, the second risk is potentially the worst. The reason for this view is that Government knows about Year 2000 risks and that these can impact on the operations of organisations that it regulates. For example Y2K may pose threats to safety caused by equipment malfunctioning or failure. This area is regulated by WorkCover. WorkCover have initiated a number of strategies to make business aware of Y2K issues. These strategies include issuing of pamphlets about Y2K.

---

[56] The Audit Office would like to acknowledge the assistance of DPWS and TCO in preparing this section

Insurers Legal issues associated with the Year 2000 problem are currently being examined by the general insurance industry. The Insurance Council of Australia has informed The Audit Office that, because there are likely to be a number of insurance issues arising from the potential failure of equipment related to the millennium change:

> ... Insurers are considering the likely impact on a wide range of insurance products. This extends not only to the possible damage effect of equipment failure but to consequential financial losses and, equally important, the liabilities on those with responsibility for ensuring that systems and equipment are millennium compliant. [57]

Suppliers Legal views regarding the liability of suppliers are varied. On the one hand, there is the view that manufacturers, suppliers and maintainers of hardware and software could be liable. Consultants and bureau processing operators could also be liable.

On the other hand, there is the view that because the practice of two digit programming is widely used in the industry and widely known and accepted in the user community, liability of suppliers is not so evident.

According to Minter Ellison, current contracts and maintenance clauses (which are often renewable annually) may well provide avenues for rectification of Y2K problems. Warrantees often imply that software is fit for the task for which it is supplied and is of reasonable quality. Maintenance contracts may require the supplier to ensure that maintained software "performs to certain specifications or is available for use of the software without defects". [58]

Because of the lack of clarity on legal matters, it is essential that:

- agencies review their contracts and maintenance agreements
- legal issues be addressed at a whole of Government level through a central agencies program referred to above (see Attachment 2)

---

[57] correspondence to The Audit Office from The Insurance Council of Australia Limited, 12 August 1997.
[58] Robert Neely, "Technology and Intellectual Property: The Year 2000 Bug", 5 August 1997, p.3.

- legal issues considered include:
  - the nature and scope of risks to individual agencies, and especially regulatory bodies
  - Government liability
  - directors responsibilities under *Corporations Law*[59]
  - intellectual property considerations
  - tenders and contract management issues.

5.6 Contract Management

A major avenue for achieving Year 2000 compliance is through management of existing or new contracts. Effective and efficient management of contracts and suppliers requires that:

- a standardised Year 2000 definition and compliance criteria be explicitly described in contracts and purchasing agreements

- the above definition and criteria be developed centrally

- the above definition and criteria be made available to all government agencies to incorporate into their own standards and procedures

- a conscious decision be made regarding whether all goods and services purchased by Government should have Year 2000 compliance and that there be an understanding of the implications of this requirement

- compliance status of whole of Government contracts and approved products be validated centrally and be communicated to all individual government agencies[60]

- centralised purchase be promoted where economies of scale can be achieved.

Vendor communication

Currently communication with vendors in NSW is occurring by DPWS requesting IT vendors who have products on the Government information panel and period contracts to provide a statement as to their Y2K status. The DPWS has also asked vendors for details of any planned timetable for the release of Year 2000 capable versions. This information has been made available by DPWS via the Internet.

Line agencies are also approaching vendors on an individual basis.

In other jurisdictions such as British Columbia and Western

---

[59] This issue will affect NSW public sector State Owned Corporations. While the legal position may be clear for company SOCs (water) it may not be as clear for Statutory SOCs (ports, rail and electricity).
[60] EDS, 1997, p.4.

Australia central agencies are negotiating with suppliers/industry to achieve economies of scale across the public sector. Centralised negotiations have included use of tools and purchase of commonly used software. Other possibilities might include reduced rates for use of specialist advice/use of fee based services and testing centres.

In NSW, negotiations have included the development of a period panel contract to provide Government agencies with a list of approved Year 2000 remedial contracting service providers. They will be able to provide agency executives with credible and effective remedies for Year 2000 issues, and to ensure these services are available to Government agencies in a timely and cost effective manner.

Engagements under this contract may cover the:

- implementation of a detailed Year 2000 project management plan
- design
- implementation of remedial actions
- changes
- testing
- integration
- other Year 2000 requirements determined by the agencies.

To ensure suppliers accept liability for the effectiveness of their goods and services, the NSW Government, through DPWS, is developing special contract provisions for the supply of goods and services (see 5.4).

The tender Schedule requires two commitments by the supplier to ensure that they give due consideration to this obligation. First, the supplier must give warranty that the goods and systems to be supplied are Year 2000 compliant. If it is found that the warranty is breached, the supplier will be obliged to correct the fault, and meet all costs associated with the repair. Second, the supplier must identify those goods and systems which they consider are not susceptible to the Y2K bug and provide reasons for doing so.

5.7   Financial Issues

Funding
As outlined above, it is difficult to determine the nature and level of funds needed to resolve Year 2000 problems. This is because agencies:

- are still evaluating the possible nature and extent of the problems

- have yet to decide on the nature of their resolution strategies (repair, replace etc)

- need to treat expenditure required or upgrades as part of regular IT expenditure.

Where significant replacement is needed, additional funds may be required. In the 1997-98 NSW Budget two agencies (Health and WorkCover) received significant additional funding as part of a three year program to upgrade IT.

There is no clear statement regarding levels of funding for Year 2000 problems. Treasury believes most agencies will fund resolution strategies as part of normal upgrade requirements.

A second and related issue is how expenditure on Year 2000 should be treated. The Urgent Issues Group (UIG) position is that costs relating to the modification of internal-use computer software for Year 2000 compatibility must be recognised as an expense in the period in which they occurred.[61]

If Year 2000 resolution projects *are* dependent on additional funding then the budget allocation should not await the Budget for the 1998/99 financial year. The time lag for agencies such as Case Study A places "unacceptable pressure" on the ability of agencies to "correct, test and deliver Year 2000 compliant systems within an acceptable time frame".[62]

---

[61] The UIG was established in 1994 by the Institute of Chartered Accountants in Australia, the Australian Society of Certified Practising Accountants, the Australian Accounting Standards Board and the Public Sector Accounting Standards Board.

[62] Coopers and Lybrand, 1997, p.46.

5.8   Recommendations

1. To reduce risks and costs to NSW and the NSW public sector, it is recommended that the NSW Government:

    - activate a central agencies program[63] which would provide DPWS' GIMB with expert advice and assistance (see Attachment 2)

    - adopt an adequate and consistent definition of Y2K compliance to be used in all IT and non IT tenders, contracts and purchasing arrangements

    - through DPWS maintain a strategic approach to Y2K issues. The approach should include targeting high risk agencies and functions and minimising duplication of agency effort.

2. To provide accountability to the NSW public, it is recommended the NSW Government report on the effectiveness of Y2K strategies by:

    - requiring agencies publish their risk management activities for the Y2K problem in their Annual Report

    - providing a publicly available, consolidated Y2K report prepared by central agencies which includes information on IT and non IT areas and agencies and functions at risk.

---

[63] The central agencies program was originally proposed by DPWS and endorsed by the NSW Government.

Attachments

1.   The Audit Process, Costs and Acknowledgments

Audit Objectives

The basic objective of the audit was to examine the efficiency and effectiveness of the NSW public sector in managing the Year 2000 problem.

Audit Criteria

The Audit Office reviewed Year 2000 initiatives from the following perspective:

Whole of Government

The general nature and level of risks and estimated costs to the NSW public sector of the Year 2000 problem should be identified and addressed.

Sub Criteria

The Government should ensure that there is effective and efficient management by:
- identifying agencies and areas most at risk
- co-ordinating and supporting a clearly defined whole of Government strategy
- implementing and costing resolution strategies for core business areas most at risk of Year 2000 problems
- developing and costing strategies for corporate support functions affected by Year 2000
- informing agencies about nature and risk of Year 2000 problem
- providing clear and timely guidelines on appropriate Year 2000 responses.

Individual Agencies

Agencies should have:
- management awareness of the problem
- formulated a strategy to investigate and rectify problems
- developed an inventory
- undertaken an assessment of risk and compliance in IT and non-IT areas
- developed a compliance plan and testing program.

Audit Scope

The scope included strategies at a whole of Government and agency level and which encompassed IT and non IT issues.

Audit Methodology

The audit method involved:

- reviewing the relevant literature

- undertaking two agency case studies in conjunction with the DPWS to evaluate agency risk (one agency met part costs of the case study)

- reviewing the Year 2000 strategies adopted by the DPWS

- contacted peak bodies and suppliers

- collating and analysing information regarding Year 2000 policies and strategies adopted by other jurisdictions and other audit offices.

Audit Costs

The total cost of the audit is as follows:

Direct salary and overhead costs	$125,225
Value of unpaid overtime (at standard rates only)	$18,044
Printing (estimated cost)	$7,000
Consultants	$58,500
Travel	$276
Total Cost	**$209,045**

Note Case Study Agency A contributed $13,000 toward costs of case studies.

Acknowledgments

The Audit Office acknowledges DPWS for their co-operation with the case studies and access to agency information on Year 2000 strategies. The excellent assistance of the two case study agencies, central and line agencies, other jurisdictions, industry and business, professional and peak organisations in providing information to The Audit Office is also acknowledged.

2. Proposed Membership and Functions of Central Agencies Program

Proposed Membership and Functions of Central Agencies Program

It is recommended that the NSW Government develop a central agencies program as originally proposed by DPWS to provide DPWS' GIMB with expert advice and assistance.

Membership would include agencies such as the ones originally proposed by DPWS: Premier's Department; Treasury and Crown Solicitor's. As decisions about Year 2000 issues require consideration of policy issues, it is suggested that The Cabinet Office also be included.

The functions of the central agencies program would include:

- developing and enforcing a consistent definition of Year 2000 compliance

- advising on legal and financial issues for the NSW public sector

- establishing an appropriate timeframe and milestones for implementation of Government Year 2000 strategies

- monitoring and reporting on agencies' Year 2000 compliance

- reviewing how Government businesses will report on Year 2000 compliance.

- co-ordinating an industry/small business strategy to increase awareness of risks to small business (proposed by DPWS as a separate strategy) developed by Department of State and Regional Development, Department of Fair Trading (DFT) and WorkCover

- utilising material and lessons learned from other jurisdictions in developing definitions, standards, guidelines and whole of Government advice re legal issues and approaches.

3.   Examples of Year 2000 Effects on Building Services

The NSW Fire Brigades provide the network infrastructure, monitor and initiate response on receipt of a signal from a subscriber's premise Automatic Fire Alarm (AFA) System indicating if there is a fire. This and other information is automatically presented to the Fire Brigades' Communications Centre. The Brigades do not provide the fire alarm panel, merely a connection to it.

The AFA panels are covered by Australian Standard AS 1670 and are therefore a national matter.

The NSW Fire Brigades has indicated to The Audit Office that it is unlikely that AFA reporting systems installed at required premises will be adversely affected. However, "it is quite probable that building management (including access control) and alarm systems that are not covered under AS 1670 will be effected. Correction is clearly something for manufacturers to address."[64]

Towards the end of 1997 the NSW Fire Brigades is to commence transferring AFA Monitoring Services to third party network providers and operators. This means that all AFA systems for premises required to have alarms will be transferred to the private sector. The provision of services by the private sector will be managed by way of a service level agreement. Any Year 2000 compliance problems will be addressed through this agreement and the accompanying technical specification.

Lift manufacturers may face different Year 2000 problems. One major supplier has indicated to The Audit Office that

> whilst lift operation may not generally be affected, some impact will occur. Potential problems seem to revolve around performance measuring software where string dates are used to calculate results. Some car lift displays may also have difficulty in updating from 99 to 00.[65]

Remedies for these problems will range from software changes to manipulating the equipment through the time change.

---

[64] NSW Fire Brigades letter to The Audit Office, 17 July 1997.
[65] Kone letter to The Audit Office, 18 July 1997.

In terms of communications, Telstra has indicated to The Audit Office that it has already established a corporate Year 2000 Programme. This programme aims "to scope and define changes in Telstra's environment, and to drive a controlled programme which will assist a smooth transition".[66] Telstra is currently performing technical audits on its existing products and services and has a Year 2000 plan in place. It is aiming to address the compliancy issues of its major products and services by the end of 1998. Products and services with lesser impacts will be addressed during the following year.

---

[66] Telstra correspondence to The Audit Office 21 July 1997.

4.   Commonwealth and State Strategies

Y2K Item	Commonwealth[67]	Vic[68]	SA[69]	Tas[70]	WA[71]	QLD[72]
Policy	Facilitation /compliance driven by Office of Government Information Technology, reporting to Ministers for Finance, Science Industry and Tourism and Consumer Affairs Y2K Policy[73] & national strategy established	Y2K regarded as an agency responsibility Policy and Implementation guidelines issued by Department of State and Regional Development	Cabinet decision recognised Y2K importance. Y2K individual agency responsibility. Dept. IT Services co-ordinates activities. Central agency program (Treasury, Premier's, Dept. IT Services & Attorney-General) to review overall Government impact.	Y2K an agency responsibility. Year 2000 Chapter to be included in the Guidelines for Project Management. Guidelines are distributed to all project managers across State Government. Chapter includes advice for running Year 2000 projects as well as including Year 2000 considerations in all projects. Currently awaiting ratification.	Y2K seen as CEO responsibility Y2K in CEO Performance Agreement (see CEO below)	Premier's Dept developing a set of Guidelines and Checklist in conjunction with Coopers and Lybrand and Allen Allen & Hemsley
Definition	yes	yes, in warranty	No official Y2K compliance definition published. BSI definition given to agencies.	Currently liaising with the Tasmanian Crown Solicitor's Office to produce a standard contract guidance note.	yes	yes

---

[67] Information supplied by OGIT, 24 September 1997.

[68] Information supplied by Multimedia, Victoria 19 September, 1997.

[69] Information supplied by SA Y2K Co-ordinator, 15 October 1997.

[70] Information supplied by Tasmanian Department of Premier and Cabinet, 5 November 1997.

[71] Information supplied by WA Premier's Department, 4 November 1997.

[72] Information supplied by QLD Department of Premier and Cabinet, 25 September 1997.

[73] Includes compliance plans, methodology, milestones, reporting framework.

Y2K Item	Commonwealth	Vic	SA	Tas	WA	QLD
Standards	yes	Date/time standard policy issued Sept 97 (3802.1989 Based)	Recommended Date Standard published for agencies. Conforms to AS 3802.1989 and ISO 8601.1988 as CCYYMMDD.			
Priorities	business critical systems for C'wealth agencies; establishing national strategy	Utilities Health Transport	Govt. utilities, Health, Transport plus small business sector through govt./industry co-operation		Critical business risk management in three areas: - computing - embedded chips - supply chain focus on utilities, areas with customer chains, health, Worksafe and industry	business and industry
Structure	complex reporting and accountability structure; involves industry, States and all Commonwealth agencies	within normal administrative structures	Y2K co-ordinator in each agency. Central SA Govt. Co-ordinator. Standard reporting function to Cabinet.	Within Government, Year 2000 Working Party to provide strategic direction, individual agencies have their own structures. The State Government's business development arm, Tasmanian Development and Resources, is raising awareness of the problem in the private sector.	Multi agency Year 2K Focus Group; Premier's Dept Project Team (manage Govt strategy and govt agencies); industry awareness through Dept Commerce & Trade	Information Planning Branch (Premier's Dept)

Y2K Item	Commonwealth	Vic	SA	Tas	WA	QLD
Scope	IT, non IT for C'wealth agencies	IT and non IT	IT, non IT and supply chain areas focusing on business risk, not just IT.	IT, non-IT, supply chain issues	includes: • IT • areas with embedded chips • business relationships (supply chain)	IT and non IT agency reference groups established for IT and non IT government assets
Business Enterprises	National strategy by Dept Industry, Science & Tourism $5.43m allocated in Sept 97	Small Business Victoria (Dept State Development) responsible for awareness/assistance campaign	Consortium of Business Centre (Govt. Business Arm), Chamber of Commerce, Local Govt. Association and Industry Bodies to develop awareness & solutions provision strategy for SA Business co-ordinated by SA Govt. Y2K Co-ordinator. National Strategy linkage and potential private sector funding.	Small Business Bureau contacted The State Government's business development arm, Tasmanian Development and Resources, is raising awareness of the problem in the private sector.	utilities (power, light) and areas with customer chains targeted Minister for Commerce and Trade responsible for communicating with industry through Industry Awareness Task Force	co-ordination of agencies with business & industry focus; Consumer Affairs preparing Fact Sheet on purchase of home computers and software; meetings with Dept Economic Development & Trade & peak industry bodies to determine awareness/preparedness; State strategy to be developed after consultation

Y2K Item	Commonwealth	Vic	SA	Tas	WA	QLD
Reporting	Mandatory quarterly reporting required by all C'wealth agencies through OGIT to Cabinet starting Nov 97	Ministers have sought details of portfolio Year 2000 plans by 31/12/97	Initial Cabinet reporting on milestone progress per Federal timetable. Putting in place reporting for all agencies on status of progress against identified critical compliance plan items.	No formal reporting structure to Year 2000 Working Party. Surveys conducted by Information Strategy Unit (April 1997) and Tasmanian Audit Office (October 1997).	CEO must report to Minister; agency must report in Annual Report; quarterly agency reporting against milestones	Cabinet, Information Planning Board, CEO Forum; Whole of Govt. - agency progress to be reported to Co-ordinator General[74] on a regular basis
CEO	All heads of Depts and agencies held accountable	Dept Secretaries informed of responsibilities by Department of State Development (DSD)	Agency CEOs are responsible for continuation of agency business after 2000. CEOs targeted by awareness campaign and CEO IT forum.		Y2K in CEO Performance Agreement	Co-ordinator General written to CEO's Forum re importance of Y2K work
Ideas exchange	C/S quarterly forum forums Y2K sub-committee self-help groups Y2K chat list for all govts OGIT homepage national homepage specialist monthly workshops	Y2K special Interest Group of IT directors	Agency Co-ordinator Forums bi-monthly. Newsletter and chat lists being put in place. Web site information. Distribution of agency co-ordinator contact information to all other co-ordinators.	List Server 2000 as ideas exchange WP seminars	website seminars agency based focus groups chat list being organised workshops newsletter	agency reference group meets on a monthly basis

[74] Director General of Premier's Dept. is Co-ordinator General

Y2K Item	Commonwealth	Vic	SA	Tas	WA	QLD
Information	OGIT website national website brochures	Special Interest Group provided with information by DSD	Year 2000 website. Co-ordinators Newsletter. Agency Co-ordinators forums. Essential web information to co-ordinators via fax/email. Central compliance info. planned.	WP to identify areas of common concern to agencies	website direct mail newsletter	website
Legal	Attorney General's actively involved especially in defining compliance, contract issues specific legal workshop outsourcing clauses etc	Contractual clauses provided to departments	Considering legal liability of Government for Y2K, including personal liability.	Interagency Legal Issues Group	Crown Solicitor's Office involved in compliance definition and overall legal liability definition WorkSafe looking at occ health and safety Fair Trading looking at Trade Practices Act issues	Law firm appointed to incorporate legal checkpoints in guidelines; issues-rights & remedies for reverse code, engineering code, warrantees on software, contracts to be included. Crown Law to ensure central agencies investigate exposure before taking remedial action.
Checklist	checklist established 1996		Checklist on website 1997. Process and proformas provided to agencies October 1997.	IT and non IT systems checklist to be produced by WP	checklist provided to agencies (Information Policy Council) checklist (AO) further checklists being developed	Final Guidelines and Checklist sent to agencies Sept 97

Y2K Item	Commonwealth	Vic	SA	Tas	WA	QLD
Contracts	as above Dept Admin Services rolled over all PE product contracts. Only Y2K compliant products to be listed.	Guidelines includes terms and conditions for future contracts policy issued; very detailed warranty clauses provided by Department of State Development[75]	Contractual clauses in development. Compliance clause in PC and other product panel whole of Government supply contracts.	Currently being reviewed by Legal Issues Committee, including Crown Solicitor's Office, major Treasury purchasing sections.	Y2K compliance clauses for tenders and contracts being managed by Dept Contract and Management Services (CAMS) Interagency working party assessing compliance issues	Y2K compliance clauses for orders and contracts
Expertise /tools	Approved PE68 panel of 32 Y2K service providers	MMV and Education Departments testing desktop assessment tools	Register of Y2K companies offering expertise loaded on website based on invitation to industry. Will post register of evaluation tools.		Register of Y2K service providers available on Internet Register of training providers to develop staff skills in Y2K also on Internet	
Awareness	on-going awareness campaign CEO breakfast forums non IT groups	Literature, memos etc to CEOs and IT directors	Ran Chief Executive awareness forums and some targeted CEO breakfast sessions. Letters to CEOs of all agencies and Health units.	see above Ongoing presentations upon request. Standing item on Information Technology Managers' Group agenda. Business seminars.	ongoing awareness activities and reporting	strategies for business awareness

---

[75] Department of State and Regional Development, Year 2000 Policy, July 1997,p.2.

Y2K Item	Commonwealth	Vic	SA	Tas	WA	QLD
Compliance	agencies must comply - focus on business critical systems		Agencies required to follow Federal Time Scale including Inventory, Assessment, Correction, Testing and Contingency phases. Central Monitoring and tracking of essential systems.		agencies to self manage-implemented through reporting arrangements	
AO Action	AO Survey Report due, to be tabled Dec 97.	OAG surveyed agencies 1996 Y2K now a compliance requirement	Auditor-General informed of issue by Cabinet. Agency Annual Reporting requirements now include Year 2000. Auditor-General will audit Y2K as part of regular process.	AO informed of issue by Dept Premier & Cabinet Audit Office conducted survey of Tasmanian Agencies, GBEs, local government and statutory bodies (October 1997). Will table report in late November 1997. Represented on Year 2000 Working Party.	AO provided[76]: background paper distributed to auditors and clients; risk matrix to assist agencies assess different exposures and risk management activities; standard questions to be included in compliance audit an audit conducted to assess degree to which agencies have addressed Y2K risks - outcome to be included in next Auditor-General's report.	AO to assist agencies in determining risk; AO recently asked high level Y2K questions about agency awareness.

---

[76] Office of Auditor General communication to NSW Audit Office 6 August 97 and 4 November 1997.

Performance Audit Reports

Agency or Issue Examined	Title of Performance Audit Report or Publication	Date Tabled in Parliament or Published
Department of Housing	*Public Housing Construction: Selected Management Matters*	5 December 1991
Police Service, Department of Corrective Services, Ambulance Service, Fire Brigades and Others	*Training and Development for the State's Disciplined Services:* *Stream 1 - Training Facilities*	24 September 1992
Public Servant Housing	*Rental and Management Aspects of Public Servant Housing*	28 September 1992
Police Service	*Air Travel Arrangements*	8 December 1992
Fraud Control	*Fraud Control Strategies*	15 June 1993
HomeFund Program	*The Special Audit of the HomeFund Program*	17 September 1993
State Rail Authority	*Countrylink: A Review of Costs, Fare Levels, Concession Fares and CSO Arrangements*	10 December 1993
Ambulance Service, Fire Brigades	*Training and Development for the State's Disciplined Services:* *Stream 2 - Skills Maintenance Training*	13 December 1993
Fraud Control	*Fraud Control: Developing an Effective Strategy* *(Better Practice Guide jointly published with the Office of Public Management, Premier's Department)*	30 March 1994
Aboriginal Land Council	*Statutory Investments and Business Enterprises*	31 August 1994
Aboriginal Land Claims	*Aboriginal Land Claims*	31 August 1994
Children's Services	*Preschool and Long Day Care*	10 October 1994
Roads and Traffic Authority	*Private Participation in the Provision of Public Infrastructure* *(Accounting Treatments; Sydney Harbour Tunnel; M4 Tollway; M5 Tollway)*	17 October 1994
Sydney Olympics 2000	*Review of Estimates*	18 November 1994
State Bank	*Special Audit Report: Proposed Sale of the State Bank of New South Wales*	13 January 1995
Roads and Traffic Authority	*The M2 Motorway*	31 January 1995
Department of Courts Administration	*Management of the Courts:* *A Preliminary Report*	5 April 1995
Joint Operations in the Education Sector	*A Review of Establishment, Management and Effectiveness Issues*	13 September 1995

Agency or Issue Examined	Title of Performance Audit Report or Publication	Date Tabled in Parliament or Published
	(including a Guide to Better Practice)	
Department of School Education	*Effective Utilisation of School Facilities*	29 September 1995
Luna Park	*Luna Park*	12 October 1995
Government Advertising	*Government Advertising*	23 November 1995
Performance Auditing In NSW	*Implementation of Recommendations; and Improving Follow-Up Mechanisms*	6 December 1995
Ethnic Affairs Commission	*Administration of Grants (including a Guide To Better Practice)*	7 December 1995
Department of Health	*Same Day Admissions*	12 December 1995
Environment Protection Authority	*Management and Regulation of Contaminated Sites: A Preliminary Report*	18 December 1995
State Rail Authority of NSW	*Internal Control*	14 May 1996
Building Services Corporation	*Inquiry into Outstanding Grievances*	9 August 1996
Newcastle Port Corporation	*Protected Disclosure*	19 September 1996
Ambulance Service of New South Wales	*Charging and Revenue Collection (including a Guide to Better Practice in Debtors Administration)*	26 September 1996
Department of Public Works and Services	*Sale of the State Office Block*	17 October 1996
State Rail Authority	*Tangara Contract Finalisation*	19 November 1996
NSW Fire Brigades	*Fire Prevention*	5 December 1996
State Rail	*Accountability and Internal Review Arrangements at State Rail*	19 December 1996
Corporate Credit Cards	*The Corporate Credit Card (including Guidelines for the Internal Control of the Corporate Credit Card)*	23 January 1997
NSW Health Department	*Medical Specialists: Rights of Private Practice Arrangements*	12 March 1997
NSW Agriculture	*Review of NSW Agriculture*	27 March 1997
Redundancy Arrangements	*Redundancy Arrangements*	17 April 1997
NSW Health Department	*Immunisation in New South Wales*	12 June 1997
Corporate Governance	*Corporate Governance*	17 June 1997

Agency or Issue Examined	Title of Performance Audit Report or Publication	Date Tabled in Parliament or Published
Department of Community Services and Ageing and Disability Department	*Large Residential Centres for People with a Disability in New South Wales*	26 June 1997
The Law Society Council of NSW, the Bar Council, the Legal Services Commissioner	*A Review of Activities Funded by the Statutory Interest Account*	30 June 1997
Roads and Traffic Authority	*Review of Eastern Distributor*	31 July 1997
Sydney Showground, Moore Park	*Lease to Fox Studios Australia*	December 1997
Department of Public Works and Services	*1999 - 2000 Millennium Date Rollover: Preparedness of the NSW Public Sector*	December 1997

For further information please contact:

The Audit Office of New South Wales

Street Address	**Postal Address**
Level 11	
234 Sussex Street	GPO Box 12
SYDNEY NSW 2000	SYDNEY NSW 2001
Australia	Australia

Telephone	(02)	9285 0155
Facsimile	(02)	9285 0100
Internet	http://www.audit.nsw.gov.au	
e-mail	mail@audit.nsw.gov.au	

Office Hours: 9.00am - 5.00pm Monday to Friday

Contact Officer: Stephen Horne
                             Director Performance Audit
                             +612 9285 0078

To purchase this Report please contact:

The NSW Government Information Service

Retail Shops

Sydney CBD   *Parramatta CBD*

Ground Floor	
Goodsell Building	Ground Floor
Chifley Square	Ferguson Centre
Cnr Elizabeth & Hunter Sts	130 George Street
SYDNEY NSW 2000	PARRAMATTA NSW 2150

Telephone and Facsimile Orders

Telephone

Callers from Sydney metropolitan area	9743 7200
Callers from other locations within NSW	1800 46 3955
Callers from interstate	(02) 9743 7200

Facsimile	(02) 9743 7124